Docket No. 251896US6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Yutaka NAGAO GAU:

SERIAL NO: NEW APPLICATION EXAMINER:

FILED: HEREWITH

FOR: INFORMATION PROCESSING APPARATUS, INFORMATION PROCESSING METHOD, AND INFORMATION PROCESSING SYSTEM

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2003-142593	May 20, 2003

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Registration No. 40,073

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

S04P0682US00

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　５月２０日

出願番号
Application Number: 特願２００３－１４２５９３

[ST. 10/C]: [ＪＰ２００３－１４２５９３]

出願人
Applicant(s): ソニー株式会社

２００４年　２月２３日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０１２２９１

【書類名】　特許願
【整理番号】　0390279803
【提出日】　平成15年 5月20日
【あて先】　特許庁長官　殿
【国際特許分類】　G10L　5/04
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　長尾　豊
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100067736
　【弁理士】
　【氏名又は名称】　小池　晃
【選任した代理人】
　【識別番号】　100086335
　【弁理士】
　【氏名又は名称】　田村　榮一
【選任した代理人】
　【識別番号】　100096677
　【弁理士】
　【氏名又は名称】　伊賀　誠司
【手数料の表示】
　【予納台帳番号】　019530
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置及び情報処理方法、並びに情報処理システム

【特許請求の範囲】

【請求項１】　ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置において、

第１のライセンス情報を保存する保存手段と、

第２のライセンス情報を受信する受信手段と、

第１のライセンス情報に対して第２のライセンス情報の一部又は全部を結合する結合手段とを有し、

前記結合手段により結合されたライセンス情報の範囲内でコンテンツ情報を使用することを特徴とする情報処理装置。

【請求項２】　前記第２のライセンス情報は自身が上書きのためのライセンス情報であるか、追加のためのライセンス情報であるかを識別させるライセンス識別情報を含むことを特徴とする請求項１記載の情報処理装置。

【請求項３】　前記第２のライセンス情報が上書きのためのライセンス情報であることを前記ライセンス識別情報から確認したとき、前記結合手段は前記第２のライセンス情報の一部又は全部を前記第１のライセンス情報の一部又は全部に上書きすることを特徴とする請求項２記載の情報処理装置。

【請求項４】　前記第２のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から確認したとき、前記結合手段は前記第１のライセンス情報に対して前記第２のライセンス情報の一部又は全部を追加することを特徴とする請求項２記載の情報処理装置。

【請求項５】　前記結合手段により結合されたライセンス情報に対して情報処理装置固有の鍵情報を用いて電子署名を行うことを特徴とする請求項１記載の情報処理装置。

【請求項６】　前記第１のライセンス情報及び前記第２のライセンス情報が期間制限を指定する権利内容を含み、前記第２のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から確認したとき、前記結合手段は前記第１のライセンス情報の権利内容に基づいた規則により前記第１のラ

イセンス情報と第２のライセンス情報とを結合することを特徴とする請求項２記載の情報処理装置。

【請求項７】　前記第１のライセンス情報及び前記第２のライセンス情報がフラグを指定する権利内容を含み、前記第２のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から確認したとき、前記結合手段は前記第１のライセンス情報の権利内容に基づいた規則により前記第１のライセンス情報と第２のライセンス情報とを結合することを特徴とする請求項２記載の情報処理装置。

【請求項８】　前記第１のライセンス情報及び前記第２のライセンス情報が回数を指定する権利内容を含み、前記第２のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から確認したとき、前記結合手段は前記第１のライセンス情報の権利内容に基づいた規則により前記第１のライセンス情報と第２のライセンス情報とを結合することを特徴とする請求項２記載の情報処理装置。

【請求項９】　ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能とする情報処理方法において、

第１のライセンス情報を保存する保存工程と、

第２のライセンス情報を受信する受信工程と、

前記受信工程で受信した第２のライセンス情報が上書きのためのライセンス情報であるか、追加のためのライセンス情報であるかを識別させるライセンス識別情報から上書き又は追加属性を判別する判別工程と、

前記判別工程で判別した上書き又は追加属性に応じて第１のライセンス情報に対して第２のライセンス情報の一部又は全部を結合する結合工程とを有し、

前記結合工程により結合されたライセンス情報の範囲内でコンテンツ情報を使用することを特徴とする情報処理方法。

【請求項１０】　前記判別工程が前記ライセンス識別情報から前記第２のライセンス情報が上書きのためのライセンス情報であることを判別したとき、前記結合工程は前記第２のライセンス情報の一部又は全部を前記第１のライセンス情報の一部又は全部に上書きすることを特徴とする請求項９記載の情報処理方法。

【請求項１１】　前記判別工程が前記ライセンス識別情報から前記第２のライセンス情報が追加のためのライセンス情報であることを判別したとき、前記結合手段は前記第１のライセンス情報に対して前記第２のライセンス情報の一部又は全部を追加することを特徴とする請求項９記載の情報処理方法。

【請求項１２】　前記第１のライセンス情報及び前記第２のライセンス情報が期間制限を指定する権利内容を含み、前記判別工程が前記第２のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から判別したとき、前記結合工程は前記第１のライセンス情報の権利内容に基づいた規則により前記第１のライセンス情報と第２のライセンス情報とを結合することを特徴とする請求項９記載の情報処理方法。

【請求項１３】　前記第１のライセンス情報及び前記第２のライセンス情報がフラグを指定する権利内容を含み、前記判別工程が前記第２のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から判別したとき、前記結合工程は前記第１のライセンス情報の権利内容に基づいた規則により前記第１のライセンス情報と第２のライセンス情報とを結合することを特徴とする請求項９記載の情報処理方法。

【請求項１４】　前記第１のライセンス情報及び前記第２のライセンス情報が回数を指定する権利内容を含み、前記判別工程が前記第２のライセンス情報が追加のためのライセンス情報であることを前記ライセンス識別情報から判別したとき、前記結合工程は前記第１のライセンス情報の権利内容に基づいた規則により前記第１のライセンス情報と第２のライセンス情報とを結合することを特徴とする請求項９記載の情報処理方法。

【請求項１５】　第１のライセンス情報を保存する保存手段と、第２のライセンス情報を受信する受信手段と、第１のライセンス情報に対して第２のライセンス情報の一部又は全部を結合する結合手段とを有し、前記結合手段により結合されたライセンス情報の範囲内でコンテンツ情報を使用するクライアントと、

前記クライアントからの要求に応じて前記第２のライセンス情報をネットワークを通して送信するサーバと

を備えることを特徴とする情報処理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置及び情報処理方法並びに情報処理システムに関し、特に著作権者から付与されるライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置及び情報処理方法並びに情報処理システムに関する。

【０００２】

【従来の技術】

インターネット等のネットワークを経由して、音楽・映像等のディジタルコンテンツを購入するサービスが普及している。例えば、インターネットを利用した音楽配信サービス（Electronic Music Distribution：ＥＭＤ）を利用すれば、ディジタル音楽コンテンツをダウンロードしてクライアント端末であるパーソナルコンピュータに保存し、パーソナルコンピュータ上で聞くことができる。

【０００３】

このとき、パーソナルコンピュータ側では、所定の著作権保護技術を採用した音楽記録再生アプリケーションをＯＳの基に起動し、暗号化したディジタルコンテンツを含むコンテンツファイルとそれに対応する利用条件を記述した権利ファイルをＨＤＤ等に格納してセキュアなサービスを実現していた。

【０００４】

本件出願人による特開平１４－３５９６１６号公報には、所定の著作権保護技術を採用した音楽記録再生アプリケーションを起動することによってコンテンツの流通を妨げることなく、不正に利用されることを確実に防止することを目的とした情報処理装置等が開示されている。

【０００５】

【特許文献１】

特開平１４－３５９６１６号

【０００６】

【発明が解決しようとする課題】

ところで、あるデジタルコンテンツに対応する権利情報は一種類とは限らず、また一種類だとしても同一デジタルコンテンツに対して、複数の権利情報ファイルを取得することが可能である。

【０００７】

クライアント内で同一デジタルコンテンツに対して複数権利情報ファイルが存在する場合、権利情報ファイルはそれぞれ独立に扱われており、権利情報ファイル同士のクライアント内での結合を行うことができなかった。そのため、権利情報ファイルはその個数分だけ存在し、ユーザが単一コンテンツを利用する場合でも、権利の選択をする必要があった。

【０００８】

本発明は、前記実情に鑑みてなされたものであり、複数権利の組み合わせによる権利表現を可能とし、より柔軟な権利表現が可能となる情報処理装置及び情報処理方法、並びに情報処理システムの提供を目的とする。

【０００９】

【課題を解決するための手段】

本発明に係る情報処理装置は、前記課題を解決するために、ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置において、第１のライセンス情報を保存する保存手段と、第２のライセンス情報を受信する受信手段と、第１のライセンス情報に対して第２のライセンス情報の一部又は全部を結合する結合手段とを有し、前記結合手段により結合されたライセンス情報の範囲内でコンテンツ情報を使用する。

【００１０】

本発明の情報処理装置は、結合手段により第１のライセンス情報に対して第２のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてコンテンツ情報を使用する。

【００１１】

本発明に係る情報処理方法は、前記課題を解決するために、ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能とする情報処理方法において、第１のライセンス情報を保存する保存工程と、第２のライセンス情報を受

信する受信工程と、前記受信工程で受信した第２のライセンス情報が上書きのためのライセンス情報であるか、追加のためのライセンス情報であるかを識別させるライセンス識別情報から上書き又は追加属性を判別する判別工程と、前記判別工程で判別した上書き又は追加属性に応じて第１のライセンス情報に対して第２のライセンス情報の一部又は全部を結合する結合工程とを有し、前記結合工程により結合されたライセンス情報の範囲内でコンテンツ情報を使用する。

【００１２】

本発明の情報処理方法は、結合工程により第１のライセンス情報に対して第２のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてコンテンツ情報を使用する。

【００１３】

本発明に係る情報処理システムは、前記課題を解決するために、第１のライセンス情報を保存する保存手段と、第２のライセンス情報を受信する受信手段と、第１のライセンス情報に対して第２のライセンス情報の一部又は全部を結合する結合手段とを有し、前記結合手段により結合されたライセンス情報の範囲内でコンテンツ情報を使用するクライアントと、前記クライアントからの要求に応じて前記第２のライセンス情報をネットワークを通して送信するサーバとを備える。

【００１４】

本発明の情報処理システムでは、クライアントの保存手段に保存されている第１のライセンス情報に対して、クライアントからの要求に応じてサーバから送信された第２のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてクライアントがコンテンツ情報を使用する。

【００１５】

以上の本発明によれば、ライセンス情報を格納している権利ファイルにクライアント内での結合属性を指定可能とするとともに、その中で指定される各種権利情報に関しても属性に応じた結合ルールを設けるので、それにより複数権利ファイルをクライアント内で結合し単一権利としての利用を可能にする。

【００１６】

【発明の実施の形態】

図１は、本発明を適用したコンテンツ提供システム１の構成を示している。コンテンツ提供システム１は、映像及び／音声データよりなるデータを扱う。サーバ１１は、インターネットのようなネットワーク２を介してクライアント１２に接続している。ここでは、クライアント１２を一台のみ図示しているが、インターネット２には、任意の台数のクライアント１２が接続される。

【００１７】

クライアント１２は、後述するライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置であり、既存（第１の）ライセンス情報を記憶部に記憶している。また、新規（第２の）ライセンス情報を通信部にて受信し、既存（第１の）ライセンス情報に対して新規（第２の）ライセンス情報の一部又は全部を結合する。この結合されたライセンス情報の範囲内でコンテンツ情報を使用する。

【００１８】

ここでいうライセンス情報の結合は、後述するライセンス情報の更新の一形態としてなされる。

【００１９】

なお、第２のライセンス情報は、自身が上書きのためのライセンス情報であるか、追加のためのライセンス情報であるかを識別可能なライセンス識別情報を含んでいる。

【００２０】

また、サーバ１１は、クライアント１２に対してコンテンツを提供するほか、上記コンテンツを利用するのに必要なライセンス情報を付与する。また、課金処理を行うこともある。

【００２１】

このコンテンツ提供システムは、詳細には図２に示すように記述することもできる。つまり、インターネット２には、クライアント１２－１，１２－２（以下、これらのクライアントを個々に区別する必要がない場合、単にクライアント１２と称する）が接続されている。もちろん、インターネット２には、前述したように任意の台数のクライアントが接続される。また、インターネット２には、ク

ライアント１２に対してコンテンツを提供するコンテンツサーバ１１－Ａ、コンテンツサーバ１１－Ａが提供するコンテンツを利用するのに必要なライセンスをクライアント１２に対して付与するライセンスサーバ１１－Ｂ、およびクライアント１２がライセンスを受け取った場合に、そのクライアント１２に対して課金処理を行う課金サーバ１１－Ｃが接続されている。

【００２２】

図３はクライアント１２の構成を表している。図３において、ＣＰＵ（Central Processing Unit）２１は、ＲＯＭ（Read Only Memory）２２に記憶されているプログラム、または記憶部２８からＲＡＭ（Random Access Memory）２３にロードされたプログラムに従って各種の処理を実行する。タイマ２０は、計時動作を行い、時刻情報をＣＰＵ２１に供給する。ＲＡＭ２３にはまた、ＣＰＵ２１が各種の処理を実行する上において必要なデータなども適宜記憶される。

【００２３】

暗号化復号部２４は、コンテンツデータを暗号化するとともに、既に暗号化されているコンテンツデータを復号する処理を行う。コーデック部２５は、例えば、ＡＴＲＡＣ（Adaptive Transform Acoustic Coding）３方式などでコンテンツデータをエンコードし、入出力インタフェース３２を介してドライブ３０に接続されている半導体メモリ４４に供給し、記録させる。あるいはまた、コーデック部２５は、ドライブ３０を介して半導体メモリ４４より読み出した、エンコードされているデータをデコードする。半導体メモリ４４は、いわゆるメモリーカードとして用いられているものである。

【００２４】

ＣＰＵ２１、ＲＯＭ２２、ＲＡＭ２３、暗号化復号部２４、およびコーデック部２５は、バス３１を介して相互に接続されている。このバス３１にはまた、入出力インタフェース３２も接続されている。

【００２５】

入出力インタフェース３２には、キーボード、マウスなどよりなる入力部２６、ＣＲＴ、ＬＣＤなどよりなるディスプレイ、並びにスピーカなどよりなる出力部２７、ハードディスクなどより構成される記憶部２８、モデム、ターミナルア

ダプタなどより構成される通信部２９が接続されている。

【００２６】

通信部２９は、インターネット２を介しての通信処理を行う。ＣＰＵ２１から提供されたデータを送信する。また通信部２９は通信相手から受信したデータをＣＰＵ２１、ＲＡＭ２３、記憶部２８に出力する。記憶部２８はＣＰＵ２１との間でやり取りし、情報の保存・消去を行う。通信部２９はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

【００２７】

入出力インタフェース３２にはまた、必要に応じてドライブ３０が接続され、磁気ディスク４１、光ディスク４２、光磁気ディスク４３、或いは半導体メモリ４４などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部２８にインストールされる。

【００２８】

なお、図示は省略するが、コンテンツサーバ１１－Ａ、ライセンスサーバ１１－Ｂ、課金サーバ１１－Ｃも、図３に示したクライアント１２と基本的に同様の構成を有するコンピュータにより構成される。そこで、以下の説明においては、図３の構成は、サーバ１１の構成としても引用される。

【００２９】

コンテンツ提供システム１にあってサーバ１１はクライアント１２に、図４に示すようにコンテンツと共にライセンス情報を送る。クライアント１２がコンテンツを再生するためにはライセンスが必要となる。

【００３０】

コンテンツは、図５に示すように、コンテンツ本体と鍵から構成され、コンテンツ本体は何重にも鍵が掛けられている。クライアント１２側では、受け取ったコンテンツとライセンス情報を基に、コンテンツ本体を復号し再生する。ライセンス情報には、使用権利UsageRightが記述されている。使用権利UsageRightは、例えばコンテンツの再生期限、再生回数、或いはＣＤ等のメディアへのコピー回数、ポータブルデバイス（ＰＤ）へのチェックアウト回数等の各種使用条件を示す情報である。

【００３１】

本実施の形態にあって、クライアント１２は、ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置であり、既存（第１の）ライセンス情報を記憶部２８に記憶している。また、新規（第２の）ライセンス情報を通信部２９にて受信する。既存（第１の）ライセンス情報に対して新規（第２の）ライセンス情報の一部又は全部をＣＰＵ２１により結合する。このＣＰＵ２１により結合されたライセンス情報の範囲内でコンテンツ情報を使用する。

【００３２】

このため、クライアント１２は、ＣＰＵ２１の制御の基に図６に示すような機能ブロックとして機能する。クライアントの通信機能１２０はサーバ１１からのメッセージを受け取り、そのメッセージを管理機能１２１に渡す。また、管理機能１２１より受け取ったメッセージをサーバ１１に送信する。暗号機能１２３は、サーバ１１と共有している秘密鍵を用いてメッセージの暗号化・復号化を行う。管理機能１２２は一部、暗号機能１２３を用いてメッセージを生成・解析する。記憶装置１２４は、前記記憶部２８に相当し、既存（第１の）ライセンス情報を記憶している。また、結合された後のラインセンス情報も記憶する。

【００３３】

サーバ１１は、ＣＰＵ２１の制御の基に図７に示すような機能ブロックにしたがって機能する。通信機能１１０はクライアント１２からのメッセージを受け取り、そのメッセージを管理機能１１１に渡す。また、管理機能１１１より受け取ったメッセージをクライアント１２に送信する。暗号機能１１３は、クライアントと共有している秘密鍵を用いてメッセージの暗号化・復号化を行う。管理機能１１１は、通信機能１１０を経由してクライアント１２とメッセージを交換し、そのメッセージに応じた処理をする。また管理機能１１１は、一部暗号機能１１３を用いてメッセージを生成・解析する。処理装置１１２は、管理機能１１１より要求のあった処理を行う。

【００３４】

次に、図８を参照して、前記ライセンス情報を格納している既存権利ファイル

と新規権利ファイルの簡略化したデータ構成を説明する。この既存権利ファイル又は新規権利ファイルのデータ構成は、一つのコンテンツ毎に設定される。また、一つのコンテンツに対して複数の権利ファイルも設定される。また、複数のコンテンツに対して一つの権利ファイルが設定されてもよい。

【００３５】

先ず、データネーム（Data Name)が記述される。その後に、ユーセージライトタイプ（Usage Right Type：使用権利タイプ）が記述されている。以下、コンテンツＩＤ（ＣＩＤ）、ユーセージライトディスジャンクションルール（Usage Right Disjunction Rules：使用権利分離規則）、リーフＩＤ（LeafＩＤ：端末ＩＤ）、ディバイスアンドメディアカテゴリーフォアチェクアウト（Devaice and Media Categories for Check Out：チェックアウトのための端末及び媒体のカテゴリー）、チェックアウトマックスカウント（Check Out Max Count：チェックアウトの最大回数）、デバイスアンドメディアカテゴリーフォアコピー（Devaice and Media Categories for copy：コピーのための端末及び媒体のカテゴリー）、コピーマックスカウント（Copy Out Max Count：コピーの最大回数）が記述されている。また、アトラック３ＣＤバーンマックスカウント（AT3CD Burn Max Count：符号化方式アトラック３でのＣＤへの複写最大回数）、スタートタイム（start_time：絶対開始時間）、エンドタイム（end_time：絶対終了時間）、ピリオドタイム（period_time：相対時間）も記述されている。これら各情報は、１つの権利ファイルの中に全て記述されている必要はなく、どれか一つ、二つ、又はそれ以外の複数でもよい。もちろん、全ての記述でも構わない。複数の場合の例としては、後述のようにチェックアウトのＰＤを指定するフラグに、その回数を指定する回数情報が付随しているような場合である。

【００３６】

ユーセージライトタイプ（UsageRightType）には、当該既存権利ファイル又は新規権利ファイルが上書き属性であるか追加属性であるかを識別させるフラグが記述されている。さらに、この使用権利タイプUsageRightTypeには、新規権利ファイルが期間制限を指定する権利内容を含む場合に、新規権利の相対期間を既存権利の絶対期間にどのように結合するかを決定する識別フラグも記述されている

。

【００３７】

コンテンツＩＤは、この権利ファイル（既存権利又は新規権利ファイル）がどのコンテンツに対応しているかを示す識別コードである。同じＩＤ、すなわちこのコンテンツはどの権利ファイルに対応するかを示す識別コードはコンテンツファイルの中にも記述されている。もちろん、改竄されないように署名がついている。

【００３８】

ユーセージライトディスジャンクションルール（Usage Right Disjunction Rules）は、フラグによって可否で規定できるルールを相関なしに独立に記述している。つまり、この領域内に独立な条件をいくつか指定している。例えば、この領域に４バイト（byte）確保している。具体的には、ビット０（bit０）をビットレートの変換の可否に規定することができる。残りのビット１－３２をリザーブ（Reserved）として、今後、可否だけを指定するようなルールの記述に用いる。

【００３９】

リーフＩＤ（LeafＩＤ）は、個々のデバイスの識別番号である。

【００４０】

ディバイスアンドメディアカテゴリーフォアチェクアウト（Devaice and Media Categories for Check Out）は、クライアントからチェックアウト可能な機器を指定するために記述されている。チェックアウトは、クライアントからポータブル機器（ＰＤ）にコンテンツを転送することを意味する。よって、クライアントからコンテンツを転送できるポータブル機器を示すフラグである。例えば、インターネットに接続して音楽データを記録できるネット接続型のミニディスク記録再生装置、時計を有してタイマー機能を備えるポータブル機器、時計のないポータブル機器の３つのカテゴリを定義できる。チェックアウト可能であることをフラグ“１”で示すと、“１１０”は、クライアントからコンテンツを転送することができるＰＤは、ネット接続型のミニディスク記録再生装置とタイマー機能を備えるポータブル機器であることを指定していることになる。時計のないポー

タブル機器にはチェックアウトできないことを意味する。なお、チェックアウトしたコンテンツをＰＤから元のクライアントに戻すことをチェックインという。クライアントからＰＤに一度チェックアウトしたコンテンツをチェックインによりまたクライアントに戻した後、再びチェックアウトすることも可能である。

【００４１】

チェックアウトマックスカウント（Check Out Max Count）は、前記ディバイスアンドメディアカテゴリーフォアチェクアウト（Devaice and Media Categories for Check Out）にてチェックアウトを許可したポータブル機器に対して最大何回までチェックアウトできるかを示す回数指定の情報である。

【００４２】

デバイスアンドメディアカテゴリーフォアコピー（Devaice and Media Categories for copy）は、クライアントからコピー可能な機器を指定するために記述されている。コピーは、クライアントからポータブル機器（ＰＤ）にコンテンツを複写することを意味する。よって、クライアントからコンテンツを複写できるポータブル機器を示すフラグである。前記ディバイスアンドメディアカテゴリーフォアチェクアウト（Devaice and Media Categories for Check Out）にて説明したのと同様に、ミニディスク記録再生装置、時計を有してタイマー機能を備えるポータブル機器、時計のないポータブル機器の３つのカテゴリを定義できる。コピー可能であることをフラグ“１”で示すと、“１１０”は、クライアントからコンテンツをコピーすることができるＰＤは、ネット接続型のミニディスク記録再生装置とタイマー機能を備えるポータブル機器であることを指定していることになる。時計のないポータブル機器にはコピーを禁止している。

【００４３】

コピーマックスカウント（Copy Out Max Count）は、前記デバイスアンドメディアカテゴリーフォアコピー（Devaice and Media Categories for copy）にてコピーを許可したポータブル機器に対して最大何回までコピーできるかを示す回数指定の情報である。

【００４４】

アトラック３ＣＤバーンマックスカウント（AT3CD Burn Max Count）は、コー

デック方式ＡＴＲＡＣ３によるＣＤへのコンテンツの複写最大回数を指定する情報である。

【００４５】

スタートタイム（start_time：絶対開始時間）はコンテンツの利用可能開始絶対日時を示し、エンドタイム（end_time：絶対終了時間）はコンテンツの利用可能終了絶対日時を示す。よって、スタートタイム（start_time：絶対開始時間）とエンドタイム（end_time：絶対終了時間）により、コンテンツの利用できる絶対期間を指定する。

【００４６】

ピリオドタイム（period_time：相対時間）は、ある特定の日時からどれくらいの期間コンテンツを利用できるかを示す情報である。

【００４７】

以上の各情報を分類すると、期間制限を指定する情報と、フラグを指定する情報と、回数を指定する情報とに分けられる。期間制限を指定する情報は、スタートタイム（start_time：絶対開始時間）とエンドタイム（end_time：絶対終了時間）とピリオドタイム（period_time：相対時間）である。

【００４８】

フラグを指定する情報は、ユーセージライトディスジャンクションルール（Usage Right Disjunction Rules）とディバイスアンドメディアカテゴリーフォアチェクアウト（Devaice and Media Categories for Check Out）とデバイスアンドメディアカテゴリーフォアコピー（Devaice and Media Categories for copy）である。

【００４９】

回数を指定する情報は、チェックアウトマックスカウント（Check Out Max Count）とコピーマックスカウント（Copy Out Max Count）とアトラック３ＣＤバーンマックスカウント（AT3CD Burn Max Count）である。

【００５０】

以上に説明したライセンス情報の既存又は新規権利ファイルは、それぞれ前記ユーセージライトタイプ（Usage Right Type）のフラグにより、上書き属性であ

るか、追加属性であるが識別される。上書き属性は、既存権利ファイルに新規権利ファイルが結合されるとき（例えば権利ファイルの更新の際に）、既存権利ファイルの内容の上に新規権利ファイルのライセンス情報を上書きしてしまうという属性を示す。追加属性は、既存権利ファイルに新規権利ファイルが結合されるとき（例えば権利ファイルの更新の際に）、既存権利ファイルのライセンス情報に新規ファイルのライセンス情報を追加するという属性を示す。

【００５１】

以下、クライアント１２が既に所有している一つの既存権利ファイルに、ライセンスサーバ１１－Ｂから新規権利ファイルを結合する際のいくつかの処理を、実施例１、実施例２、実施例３、実施例４として説明する。

【００５２】

実施例１

クライアント１２は、ライセンスサーバ１１－Ｂから送信された新規権利の属性を、前記ユーセージライトタイプ（Usage Right Type）のフラグにより、確認する。前記フラグの確認により、新規権利の属性が上書き属性である場合、既存権利で指定する全ての権利情報を新規権利の内容で書き換える。また、クライアント１２が内部的に保持している既存権利に対する状態情報（現在利用状況）も消去する。

【００５３】

前記ユーセージライトタイプ（Usage Right Type）のフラグの確認により、新規権利の属性が追加属性の場合、クライアント１２における既存権利の情報は失われることなく、値が規則に従い追加される。また、クライアント１２が内部的に保持している既存権利に対する状態情報（現在利用状況）は保持され、結合により生成された権利に対する状態情報として処理される。

【００５４】

実施例２

クライアント１２による、前記ユーセージライトタイプ（Usage Right Type）のフラグの確認により、ライセンスサーバ１１－Ｂから送信された新規権利の属性が追加属性であり、その権利情報として、前記期間制限を指定する権利内容を

含む際、新規権利と既存権利が含む前提条件に応じて下記のような結合規則が適応される。

【００５５】

先ず、結合規則２－１（実施例２の１番目の結合規則）は以下のようになる。前提条件としては、既存権利が前記スタートタイム（start_time：絶対開始時間）とエンドタイム（end_time：絶対終了時間）により、絶対期間を指定するものであり、また新規権利も絶対期間を指定するときである。この場合、結合規則２－１としては、開始期限については、既存権利と新規権利双方の開始期限を比較し、日時が小さい方を結合結果の開始期限として採用する。但し、期限のどちらかが無期限を指定する場合、無期限を採用することとする。また、終了期限について、既存権利と新規権利双方の終了期限を比較し、日時が多きい方を結合結果の終了期限として採用する。但し、期限のどちらかが無期限を指定する場合、無期限を採用することとする。

【００５６】

次に、結合規則２－２（実施例２の２番目の結合規則）は以下のようになる。前提条件としては、既存権利が前記絶対期間を指定するものであり、新規権利が前記ピリオドタイム（period_time：相対時間）により相対期間を指定するときである。この場合の結合規則２－２としては、新規権利での相対期間の追加の足し算ルールによって、ケース１とケース２に分けることになる。このケース１とケース２の識別のためのフラグも、前記ユーセージライトタイプ（Usage Right Type）に記述されている。例えば、（Usage Right Type）の何ビット目かが“１”であるか否かによって識別させる。結合規則２－２のケース１は、新規権利の相対期間の開始日時をコンテンツデータのダウンロード日時とし、終了日時を前記開始日時に相対期間を足して算出し、相対期間による開始日時及び終了日時と、既存権利の開始日時及び終了日時とを比較し、開始日時については早い方を選択し、終了日時については遅い方を選択する。結合規則２－２のケース２は、相対期間の開始日時を既存権利の終了日時とする。もしも、既存権利の終了日が過ぎてしまっている場合には、相対期間の開始日時をダウンロード時とし、終了日時はその開始日時に相対期間を足した日時とする。

【００５７】

以上の結合規則２－１と結合規則２－２にしたがった期間の決定処理手順を図９に示す。既存権利はいずれも絶対期間である。ステップＳ２０１にてクライアント１２は、ライセンスサーバ１１－Ｂから送られた新規権利の権利ファイルの前記ユーセージライトタイプ（Usage Right Type）のフラグをチェックし、追加属性であるか、上書き属性であるかを確認する。上書き属性であれば、ステップＳ２０２に進んで、既存権利に新規権利を上書きする。

【００５８】

ステップＳ２０１のチェックにて追加属性を確認すると、ステップＳ２０３に進んで新規権利の期間指定を判定する。これは、新規権利ファイルに記述されているのがスタートタイム（start_time：絶対開始時間）とエンドタイム（end_time：絶対終了時間）であるのか、或いはピリオドタイム（period_time：相対時間）であるのかをチェックすることによって判定できる。ステップＳ２０４にて判定の結果、絶対期間を指定するものであることを確認すると、ステップＳ２０５に進み、既存権利と新規権利の開始日時と終了日時を比較する。そして、ステップＳ２０６にて開始日時として早い方を選択し、また終了日時として遅い方を選択する。

【００５９】

ステップＳ２０４の判定の結果、新規権利の期間指定が相対期間を指定するものであるときには、ステップＳ２０７に進んで相対期間指定での足し算ルールの判定を、前記ユーセージライトタイプ（Usage Right Type）のフラグをチェックすることによって行う。前記フラグのチェックによりステップＳ２０８にてケース１であることを確認すると、ステップＳ２０９に進み、新規権利の相対期間の開始日時をコンテンツデータのダウンロード日時とし、終了日時を前記開始日時に相対期間を足して算出する。ステップＳ２１０では、相対期間による開始日時及び終了日時と、既存権利の開始日時及び終了日時とを比較する。そして、ステップＳ２１１にて開始日時については早い方を選択し、終了日時については遅い方を選択する。

【００６０】

ステップＳ２０８にてケース２であることを確認すると、ステップＳ２１２に進み、既存権利の絶対期間の終了日時の有効性を判定する。ステップＳ２１３では、有効であるか無効であるかをチェックし、有効であることを確認できればステップＳ２１４に進んで、既存権利の終了日時を、起点として終了日時を算出する。ステップＳ２１３にて無効であることを確認すると、既存権利の終了日が過ぎてしまっていることになるので、ステップＳ２１５にて相対期間の開始日時をダウンロード時とし、終了日時はその開始日時に相対期間を足した日時とする。

【００６１】

次に、結合規則２－３（実施例２の３番目の結合規則）は、以下のようになる。前提条件としては、既存権利が前記相対期間を指定するものであり、新規権利が前記絶対期間を指定するときである。この場合の結合規則２－３としては、開始期限については、既存権利と新規権利双方の開始期限を比較し、日時が小さい方を結合結果の開始期限として採用する。但し、期限のどちらかが無期限を指定する場合、無期限を採用することとする。終了期限について、既存権利と新規権利双方の終了期限を比較し、日時が多きい方を結合結果の終了期限として採用する。但し、どちらかの期限が無期限を指定する場合、無期限を採用することとする。

【００６２】

次に、結合規則２－４（実施例２の４番目の結合規則）は、以下のようになる。前提条件としては、既存権利及び新規権利とも相対期間を指定するときである。この結合規則２－４は、開始期限については、既存権利と新規権利双方の開始期限を比較し、日時が小さい方を結合結果の開始期限として採用する。但し、期限のどちらが無期限を指定する場合、無期限を採用することとする。終了期限について、既存権利と新規権利双方の開始期限に新規権利の相対期間で指定される期間を加算した結果を、既存権利の終了期限と比較する。計算結果が既存権利より大きければ、その値を結合結果の終了期限として採用する。計算結果が既存権利より小さければ、既存権利の終了期限を結合結果の終了期限として採用する。

【００６３】

実施例３

クライアント１２による、前記ユーセージライトタイプ（Usage Right Type）のフラグの確認により、ライセンスサーバ１１－Ｂから送信された新規権利の属性が追加属性であり、その権利情報として、前記ユーセージライトディスジャンクションルール（Usage Right Disjunction Rules）とディバイスアンドメディアカテゴリーフォアチェクアウト（Devaice and Media Categories for Check Out）とデバイスアンドメディアカテゴリーフォアコピー（Devaice and Media Categories for copy）のように、フラグを指定する権利内容を含む際には、結合規則としては、既存権利と新規権利で対応するフラグ値の論理和を計算し、その値を結合結果のフラグ値として採用する。

【００６４】

例えば、ディバイスアンドメディアカテゴリーフォアチェクアウト（Devaice and Media Categories for Check Out）の具体例を挙げる。既存権利のフラグが“０１０”であり、クライアントからコンテンツをチェックアウトすることができるＰＤは、タイマー機能を備えるポータブル機器のみであるのに対して、新規権利のフラグが“１００”であり、クライアントからコンテンツをチェックアウトすることができるＰＤは、ネット接続型のミニディスク記録再生装置のみであっても、フラグの論理和は“１１０”であるので、結合の結果、ネット接続型のミニディスク記録再生装置とタイマー機能を備えるポータブル機器の両方がチェックアウト可能となる。

【００６５】

実施例４

クライアント１２による、前記ユーセージライトタイプ（Usage Right Type）のフラグの確認により、ライセンスサーバ１１－Ｂから送信された新規権利の属性が追加属性であり、その権利情報として、回数を指定する権利内容を含む際、新規権利と既存権利が含む前提条件に応じて下記のような結合規則が適応される。

【００６６】

先ず、結合規則４－１（実施例４の１番目の結合規則）は以下のようになる。前提条件としては、既存権利が０以上の有限整数であり、新規権利も０以上の有

限整数であるときである。この場合、結合規則４－１としては、既存権利と新規権利双方の回数値を加算した値を、結合結果の回数値として採用する。但し、計算結果がクライアントの扱える整数の範囲を超える場合は無制限を意味するものとする。例えば、チェックアウトマックスカウント（Check Out Max Count）を具体例に挙げて説明する。既存権利がチェックアウト最大回数を「１０」とし、新規権利が「１５」とするときには、結合の結果を「２５」とする。ただし、クライアントの扱える整数が「２２」までである場合は無制限を意味するものとする。

【００６７】

次に、結合規則４－２（実施例４の２番目の結合規則）は以下のようになる。前提条件としては、既存権利が無制限であり、新規権利が０以上の有限整数であるときである。この場合、結合規則４－２としては、無制限を結合結果の回数値として採用する。

【００６８】

次に、結合規則４－３（実施例４の３番目の結合規則）は以下のようになる。前提条件としては、既存権利が０以上の有限整数であり、新規権利が無制限であるときである。この場合、結合規則４－３としては、無制限を結合結果の回数値として採用する。

【００６９】

次に、結合規則４－４（実施例４の４番目の結合規則）は以下のようになる。前提条件としては、既存権利及び新規権利とも無制限であるときである。この場合、結合規則４－４としては、無制限を結合結果の回数値として採用する。

【００７０】

なお、クライアント１２の要求によりサーバ１１から権利ファイルを送るときには、サーバ１１はサーバ１１のみが持つ署名用秘密鍵（PrivateKey）により署名している。そして、権利ファイル＋サーバの証明書＋署名の形式でクライアント１２に送信される。クライアント１２は公開されているサーバの公開鍵（PublicKey）で署名を復号し、復号結果が権利ファイルと一致するかどうかで権利ファイルに不正が行われていないかどうかを検証する。

【００７１】

ここで、既存権利ファイルにも新規権利ファイルにもサーバ１１による署名が付加されている。権利ファイル全部ではなく、一部の条件のみを書き換え、または追加した場合にはクライアントは、サーバのみが持つ署名用秘密鍵（PrivateKey）を持っていないのでサーバ１１と同じ署名はできない。そこで、クライアント１２は、以下のようにして結合ファイルを安全に保存する。すなわち、各々の権利ファイルについてサーバの署名を検証した後、結合した権利ファイルをクライアントのみが持つ署名用秘密鍵（PrivateKey）で署名して保存する。

【００７２】

以上に説明した実施例１～実施例４を含め、本実施の形態のコンテンツ提供システムによれば、既存の権利表現に比べ、複数権利の組み合わせによる権利表現が可能になり、より柔軟な権利表現が可能となる。

【００７３】

次に、図１０のフローチャートを参照して、クライアント１２がコンテンツサーバ１１－Ａからコンテンツの提供を受ける処理の詳細について説明する。

【００７４】

ユーザが、入力部２６を操作することでコンテンツサーバ１１－Ａに対するアクセスを指令すると、ＣＰＵ２１は、管理機能１２１によりステップＳ１において、通信機能１２０である通信部２９を制御し、インターネット２を介してコンテンツサーバ１１－Ａにアクセスさせる。ステップＳ２において、ユーザが、入力部２６を操作して、提供を受けるコンテンツを指定すると、ＣＰＵ２１は、管理機能部１２１はこの指定情報を受け取り、通信部２９から、インターネット２を介してコンテンツサーバ１１－Ａに、指定されたコンテンツを通知する。図１１のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ１１－Ａは、暗号化されたコンテンツデータを送信してくるので、ステップＳ３において、ＣＰＵ２１は、通信部２９を介して、このコンテンツデータを受信すると、ステップＳ４において、その暗号化されているコンテンツデータを記憶部２８を構成するハードディスクに供給し、記憶させる。

【００７５】

次に、図１１のフローチャートを参照して、クライアント１２の以上の処理に対応するコンテンツサーバ１１－Ａのコンテンツ提供処理について説明する。なお、以下の説明において、図３のクライアント１２の構成は、コンテンツサーバ１１－Ａの構成としても引用される。

【００７６】

ステップＳ２１において、コンテンツサーバ１１－ＡのＣＰＵ２１は、インターネット２から通信部２９を介してクライアント１２よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップＳ２２に進み、クライアント１２から送信されてきたコンテンツを指定する情報を取り込む。このコンテンツを指定する情報は、クライアント１２が、図１０のステップＳ２において通知してきた情報である。

【００７７】

ステップＳ２３において、コンテンツサーバ１１－ＡのＣＰＵ２１は、記憶部２８に記憶されているコンテンツデータの中から、ステップＳ２２の処理で取り込まれた情報で指定されたコンテンツを読み出す。ＣＰＵ２１は、ステップＳ２４において、記憶部２８から読み出されたコンテンツデータを、暗号化復号部２４に供給し、コンテンツキーＫｃを用いて暗号化させる。

【００７８】

記憶部２８に記憶されているコンテンツデータは、コーデック部２５により、既にＡＴＲＡＣ３方式によりエンコードされているので、このエンコードされているコンテンツデータが暗号化されることになる。

【００７９】

なお、もちろん、記憶部２８に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップＳ２４の処理は省略することが可能である。

【００８０】

次に、ステップＳ２５において、コンテンツサーバ１１－ＡのＣＰＵ２１は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されているコンテンツを復号するのに必要なキー情報と、コンテンツを利用す

るのに必要なライセンスを識別するためのライセンスＩＤを付加する。そして、ステップＳ２６において、コンテンツサーバ１１－ＡのＣＰＵ２１は、ステップＳ２４の処理で暗号化したコンテンツと、ステップＳ２５の処理でキーとライセンスＩＤを付加したヘッダとをフォーマット化したデータを、通信部２９から、インターネット２を介して、アクセスしてきたクライアント１２に送信する。

【００８１】

図１２は、このようにして、コンテンツサーバ１１－Ａからクライアント１２にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ（Header）とデータ（Data）とにより構成される。

【００８２】

ヘッダには、コンテンツ情報（Content information）、デジタル権利管理情報（ＤＲＭ（Digital Right Management） information）、ライセンスＩＤ（License ID）、イネーブリングキーブロック（有効化キーブロック）（ＥＫＢ（EnablingKey Block））および、ＥＫＢから生成されたキーK_{EKBC}を用いて暗号化されたコンテンツキーKcしてのデータK_{EKBC}（Kc）が配置されている。

【００８３】

コンテンツ情報には、データとしてフォーマット化されているコンテンツデータを識別するためのコンテンツＩＤ（ＣＩＤ）、そのコンテンツのコーデックの方式などの情報が含まれている。

【００８４】

デジタル権利管理情報ＤＲＭには、コンテンツを使用するための使用権利（Usage righ/rules/status）、ＵＲＬ（Uniform Resource Locator）が配置されている。使用する権利には、図８に示したように、例えば、再生期限、コンテンツの再生回数、コピー回数、チェックアウト回数などが記述される。

【００８５】

ＵＲＬは、ライセンスＩＤで規定されるライセンスを取得するときアクセスするアドレス情報であり、図２のシステムの場合、具体的には、ライセンスを受け

るために必要なライセンスサーバ１１－Ｂのアドレスである。ライセンスＩＤは、データとして記録されているコンテンツを利用するとき必要とされるライセンスを識別するものである。

【００８６】

データは、任意の数の暗号化ブロック（Encryption Block）により構成される。各暗号化ブロックは、イニシャルベクトル（ＩＶ（Initial Vector））、シード（Seed）、およびコンテンツデータをキーＫ'cで暗号化したデータＥＫ'c(data)により構成されている。

【００８７】

キーＫ'cは、次式により示されるように、コンテンツキーKcと、乱数で設定される値Seedをハッシュ関数に適用して演算された値により構成される。

K'c＝Hash(Kc, Seed)

イニシャルベクトルＩＶとシードSeedは、各暗号化ブロック毎に異なる値に設定される。

【００８８】

この暗号化は、コンテンツのデータを８バイト単位で区分して、８バイト毎に行われる。後段の８バイトの暗号化は、前段の８バイトの暗号化の結果を利用して行われるＣＢＣ（Cipher Block Chaining）モードで行われる。

【００８９】

ＣＢＣモードの場合、最初の８バイトのコンテンツデータを暗号化するとき、その前段の８バイトの暗号化結果が存在しないため、最初の８バイトのコンテンツデータを暗号化するときは、イニシャルベクトルＩＶを初期値として暗号化が行われる。

【００９０】

このＣＢＣモードによる暗号化を行うことで、１つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

【００９１】

以上のようにして、クライアント１２は、コンテンツサーバ１１－Ａからコンテンツを取得することができる。

【００９２】

この取得したコンテンツの再生には、前記図８に示したようなライセンス情報を保持している必要がある。先ず、図１３を参照して、クライアント１２がコンテンツを再生する場合の処理について説明する。

【００９３】

ステップＳ４１において、クライアント１２のＣＰＵ２１は、ユーザが入力部２６を操作することで指示したコンテンツの識別情報（ＣＩＤ）を取得する。この識別情報は、例えば、コンテンツのタイトルや、記憶されている各コンテンツ毎に付与されている番号などにより構成される。

【００９４】

そして、ＣＰＵ２１は、コンテンツが指示されると、そのコンテンツに対応するライセンスＩＤ（そのコンテンツを使用するのに必要なライセンスのＩＤ）を読み取る。このライセンスＩＤは、図１２に示されるように、暗号化されているコンテンツデータのヘッダに記述されているものである。

【００９５】

次に、ステップＳ４２に進み、ＣＰＵ２１は、ステップＳ４１で読み取られたライセンスＩＤに対応するライセンスが、クライアント１２により既に取得され、記憶部２８に記憶されているか否かを判定する。まだ、ライセンスが取得されていない場合には、ステップＳ４３に進み、ＣＰＵ２１は、ライセンス取得処理を実行する。このライセンス取得処理の詳細は、図１４のフローチャートを参照して後述する。

【００９６】

ステップＳ４２において、ライセンスが既に取得されていると判定された場合、または、ステップＳ４３において、ライセンス取得処理が実行された結果、ライセンスが取得された場合、ステップＳ４４に進み、ＣＰＵ２１は、取得されているライセンスは有効期限内のものであるか否かを判定する。ライセンスが有効期限内のものであるか否かは、ライセンスの内容として規定されている期限と、タイマ２０により計時されている現在日時と比較することで判断される。ライセンスの有効期限が既に満了していると判定された場合、ＣＰＵ２１は、ステップ

Ｓ４５に進み、ライセンス更新処理を実行する。このライセンス更新処理の詳細は、後述のフローチャートを参照して後述する。

【００９７】

ステップＳ４４において、ライセンスはまだ有効期限内であると判定された場合、または、ステップＳ４５において、ライセンスが更新された場合、ステップＳ４６に進み、ＣＰＵ２１は、暗号化されているコンテンツデータを記憶部２８から読み出し、ＲＡＭ２３に格納させる。そして、ステップＳ４７において、ＣＰＵ２１は、ＲＡＭ２３に記憶された暗号化ブロックのデータを、図１２のデータに配置されている暗号化ブロック単位で、暗号化復号部２４に供給し、コンテンツキーＫｃを用いて復号させる。

【００９８】

コンテンツキーＫｃを得る方法の具体例は、デバイスノードキー（ＤＮＫ）を用いて、ＥＫＢ（図１２）に含まれるキーK_{EKBC}を得ることができ、そのキーK_{EKBC}を用いて、データK_{EKBC}（Ｋｃ）（図１２）から、コンテンツキーＫｃを得ることができる。

【００９９】

ＣＰＵ２１は、さらに、ステップＳ４８において、暗号化復号部２４により復号されたコンテンツデータをコーデック部２５に供給し、デコードさせる。そして、コーデック部２５によりデコードされたデータを、ＣＰＵ２１は、入出力インタフェース３２から出力部２７に供給し、Ｄ／Ａ変換させ、スピーカから出力させる。

【０１００】

次に、図１４のフローチャートを参照して、図１３のステップＳ４３で行われるライセンス取得処理の詳細について説明する。

【０１０１】

クライアント１２は、事前にライセンスサーバ１１－Ｂに登録することにより、リーフＩＤ、ＤＮＫ（Device Node Key）、クライアント１２の秘密鍵・公開鍵のペア、ライセンスサーバの公開鍵、及び各公開鍵の証明書を含むサービスデータを取得しておく。

【０１０２】

リーフＩＤは、クライアント毎に割り当てられた識別情報を表し、ＤＮＫは、そのライセンスに対応するＥＫＢ（有効化キーブロック）に含まれる暗号化されているコンテンツキーＫｃを復号するのに必要なデバイスノードキーである。

【０１０３】

最初にステップＳ６１において、ＣＰＵ２１は、いま処理対象とされているライセンスＩＤに対応するＵＲＬを、図１２に示すヘッダから取得する。上述したように、このＵＲＬは、やはりヘッダに記述されているライセンスＩＤに対応するライセンスを取得するときアクセスすべきアドレスである。そこで、ステップＳ６２において、ＣＰＵ２１は、ステップＳ６１で取得したＵＲＬにアクセスする。具体的には、通信部２９によりインターネット２を介してライセンスサーバ１１－Ｂにアクセスが行われる。このとき、ライセンスサーバ１１－Ｂは、クライアント１２に対して、購入するライセンス（コンテンツを使用するのに必要なライセンス）を指定するライセンス指定情報、並びにユーザＩＤとパスワードの入力を要求してくる（後述する図１６のステップＳ１０２）。ＣＰＵ２１は、この要求を出力部２７の表示部に表示させる。ユーザは、この表示に基づいて、入力部２６を操作して、ライセンス指定情報、ユーザＩＤ、およびパスワードを入力する。なお、このユーザＩＤとパスワードは、クライアント１２のユーザが、インターネット２を介してライセンスサーバ１１－Ｂにアクセスし、事前に取得しておいたものである。

【０１０４】

ＣＰＵ２１は、ステップＳ６３，Ｓ６４において、入力部２６から入力されたライセンス識別情報を取り込むとともに、ユーザＩＤとパスワードを取り込む。ＣＰＵ２１は、ステップＳ６５において、通信部２９を制御し、入力されたユーザＩＤとパスワードを、ライセンス指定情報及びサービスデータ（後述する）に含まれるリーフＩＤを含むライセンス要求をインターネット２を介してライセンスサーバ１１－Ｂに送信させる。

【０１０５】

ライセンスサーバ１１－Ｂは、ユーザＩＤとパスワード、並びにライセンス指

定情報に基づいてライセンスを送信してくる（ステップＳ１０９）か、または、条件が満たされない場合には、ライセンスを送信してこない（ステップＳ１１２）。

【０１０６】

ステップＳ６６において、ＣＰＵ２１は、ライセンスサーバ１１－Ｂからライセンスが送信されてきたか否かを判定し、ライセンスが送信されてきた場合には、ステップＳ６７に進み、そのライセンスを記憶部２８に供給し、記憶させる。

【０１０７】

ステップＳ６６において、ライセンスが送信されて来ないと判定した場合、ＣＰＵ２１は、ステップＳ６８に進み、エラー処理を実行する。具体的には、ＣＰＵ２１は、コンテンツを利用するためのライセンスが得られないので、コンテンツの再生処理を禁止する。

【０１０８】

以上のようにして、各クライアント１２は、コンテンツデータに付随しているライセンスＩＤに対応するライセンスを取得して、初めて、そのコンテンツを使用することが可能となる。

【０１０９】

なお、図１４のライセンス取得処理は、各ユーザがコンテンツを取得する前に、予め行っておくようにすることも可能である。

【０１１０】

クライアント１２に提供されるライセンスは、前記図８に示した権利ファイルを使用条件に含ませて、図１５のように示される。

【０１１１】

次に、図１６のフローチャートを参照して、図１４のクライアント１２のライセンス取得処理に対応して実行されるライセンスサーバ１１－Ｂのライセンス提供処理について説明する。なお、この場合においても、図３のクライアント１２の構成は、ライセンスサーバ１１－Ｂの構成として引用される。

【０１１２】

ステップＳ１０１において、ライセンスサーバ１１－ＢのＣＰＵ２１は、クラ

イアント１２よりアクセスを受けるまで待機し、アクセスを受けたとき、ステップＳ１０２に進み、アクセスしてきたクライアント１２に対して、ユーザＩＤとパスワード、並びに、ライセンス指定情報の送信を要求する。上述したようにして、クライアント１２から、図１４のステップＳ６５の処理で、ユーザＩＤとパスワード、リーフＩＤ並びにライセンス指定情報（ライセンスＩＤ）が送信されてきたとき、ライセンスサーバ１１－ＢのＣＰＵ２１は、通信部２９を介してこれを受信し、取り込む処理を実行する。

【０１１３】

そして、ライセンスサーバ１１－ＢのＣＰＵ２１は、ステップＳ１０３において、通信部２９から課金サーバ１１－Ｃにアクセスし、ユーザＩＤとパスワードに対応するユーザの与信処理を要求する。課金サーバ１１－Ｃは、インターネット２を介してライセンスサーバ１１－Ｂから与信処理の要求を受けると、そのユーザＩＤとパスワードに対応するユーザの過去の支払い履歴などを調査し、そのユーザが、過去にライセンスの対価の不払いの実績があるか否かなどを調べ、そのような実績がない場合には、ライセンスの付与を許容する与信結果を送信し、不払いの実績などがある場合には、ライセンス付与の不許可の与信結果を送信する。

【０１１４】

ステップＳ１０４において、ライセンスサーバ１１－ＢのＣＰＵ２１は、課金サーバ１１－Ｃからの与信結果が、ライセンスを付与することを許容する与信結果であるか否かを判定し、ライセンスの付与が許容されている場合には、ステップＳ１０５に進み、ステップＳ１０２の処理で取り込まれたライセンス指定情報に対応するライセンスを、記憶部２８に記憶されているライセンスの中から取り出す。記憶部２８に記憶されているライセンスは、あらかじめライセンスＩＤ、バージョン、作成日時、有効期限等の情報が記述されている。ステップＳ１０６において、ＣＰＵ２１は、そのライセンスに受信したリーフＩＤを付加する。さらに、ステップＳ１０７において、ＣＰＵ２１は、ステップＳ１０５で選択されたライセンスに対応づけられている使用条件を選択する。あるいはまた、ステップＳ１０２の処理で、ユーザから使用条件が指定された場合には、その使用条件

が必要に応じて、予め用意されている使用条件に付加される。ＣＰＵ２１は、選択された使用条件をライセンスに付加する。

【０１１５】

ステップＳ１０８において、ＣＰＵ２１はライセンスサーバの秘密鍵によりライセンスに署名し、これにより、図１５に示されるような構成のライセンスが生成される。

【０１１６】

次に、ステップＳ１０９に進み、ライセンスサーバ１１－ＢのＣＰＵ２１は、そのライセンス（図１５に示される構成を有する）を、通信部２９からインターネット２を介してクライアント１２に送信させる。

【０１１７】

ステップＳ１１０においてライセンスサーバ１１－ＢのＣＰＵ２１は、ステップＳ１０９の処理で、いま送信したライセンス（使用条件、リーフＩＤを含む）を、ステップＳ１０２の処理で取り込まれたユーザＩＤとパスワードに対応して、記憶部２８に記憶させる。さらに、ステップＳ１１１において、ＣＰＵ２１は、課金処理を実行する。具体的には、ＣＰＵ２１は、通信部２９から課金サーバ１１－Ｃに、そのユーザＩＤとパスワードに対応するユーザに対する課金処理を要求する。課金サーバ５は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、ライセンスの付与を要求したとしても、ライセンスを受けることができないことになる。

【０１１８】

すなわち、この場合には、課金サーバ１１－Ｃからライセンスの付与を不許可とする与信結果が送信されてくるので、ステップＳ１０４からステップＳ１１２に進み、ＣＰＵ２１は、エラー処理を実行する。具体的には、ライセンスサーバ１１－ＣのＣＰＵ２１は、通信部２９を制御してアクセスしてきたクライアント１２に対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了させる。

【０１１９】

この場合、上述したように、そのクライアント１２はライセンスを受けることができないので、そのコンテンツを利用すること（暗号を復号すること）ができないことになる。

【０１２０】

図１７は、図１３のステップＳ４５におけるライセンス更新処理の詳細を表している。図１７のステップＳ１３１乃至ステップＳ１３５の処理は、図１５のステップＳ６１乃至ステップＳ６５の処理と基本的に同様の処理である。ただし、ステップＳ１３３において、ＣＰＵ２１は、購入するライセンスではなく、更新するライセンスのライセンスＩＤを取り込む。そして、ステップＳ１３５において、ＣＰＵ２１は、ユーザＩＤとパスワードとともに、更新するライセンスのライセンスＩＤを、ライセンスサーバ１１－Ｂに送信する。

【０１２１】

ステップＳ１３５の送信処理に対応して、ライセンスサーバ１１－Ｂは、後述するように、使用条件を提示してくる（図１８のステップＳ１５３）。そこで、クライアント１のＣＰＵ２１は、ステップＳ１３６において、ライセンスサーバ１１－Ｂからの使用条件の提示を受信し、これを出力部２７に出力し、表示させる。ユーザは、入力部２６を操作して、この使用条件の中から所定の使用条件を選択したり、所定の使用条件を新たに追加したりする。ステップＳ１３７でＣＰＵ２１は、以上のようにして選択された使用条件（ライセンスを更新する条件）を購入するための申し込みをライセンスサーバ１１－Ｂに送信する。この申し込みに対応して、後述するようにライセンスサーバ１１－Ｂは、最終的な使用条件を送信してくる（図１８のステップＳ１５４）。そこで、ステップＳ１３８において、クライアント１のＣＰＵ２１は、ライセンスサーバ１１－Ｂからの使用条件を取得し、ステップＳ１３９において、その使用条件を記憶部２８にすでに記憶されている対応するライセンスの使用条件として更新する。

【０１２２】

図１８は、以上のクライアント１２のライセンス更新処理に対応して、ライセンスサーバ１１－Ｂが実行するライセンス更新処理を表している。

最初に、ステップＳ１５１において、ライセンスサーバ１１－ＢのＣＰＵ２１

は、クライアント１２からのアクセスを受けると、ステップＳ１５２において、クライアント１２がステップＳ１３５で送信したライセンス指定情報をライセンス更新要求情報とともに受信する。

【０１２３】

ステップＳ１５３において、ＣＰＵ２１は、ライセンスの更新要求を受信すると、そのライセンスに対応する使用条件（更新する使用条件）を、記憶部２８から読み出し、クライアント１２に送信する。

【０１２４】

この提示に対して、上述したように、クライアント１２から使用条件の購入が図１７のステップＳ１３７の処理で申し込まれると、ステップＳ１５４において、ライセンスサーバ１１－ＢのＣＰＵ２１は、申し込まれた使用条件に対応するデータを生成し、ステップＳ１５４において、クライアント１２に送信する。クライアント１２は、上述したように、ステップＳ１３９の処理で受信した使用条件を用いて、すでに登録されているライセンスの使用条件を更新する。

なお、本発明の情報処理装置が適用されるクライアントは、いわゆるパーソナルコンピュータ以外に、携帯情報端末（Personal Digital Assistants：ＰＤＡ）、携帯電話機、ゲーム端末機などとすることができる。

【０１２５】

一連の処理をソフトウエアにより実行させる場合には、そのソフトウエアを構成するプログラムが、専用のハードウエアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【０１２６】

この記録媒体は、図３に示されるように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク４１（フロッピディスクを含む）、光ディスク４２（CD-ROM(Compact Disk - Read Only Memory),DVD(Digital Versatile Disk)を含む）、光磁気ディスク４３（ＭＤ（Mini-Disk）を含む）、もしくは半導体メモリ４４などよりなるパッケージ

メディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているＲＯＭ２２や、記憶部２８に含まれるハードディスクなどで構成される。

【０１２７】

また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【０１２８】

【発明の効果】

本発明に係る情報処理装置は、結合手段により第１のライセンス情報に対して第２のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてコンテンツ情報を使用するので、既存の権利表現に比べ、複数権利の組み合わせによる権利表現が可能になり、より柔軟な権利表現を可能とする。

【０１２９】

本発明に係る情報処理方法は、結合工程により第１のライセンス情報に対して第２のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてコンテンツ情報を使用するので、既存の権利表現に比べ、複数権利の組み合わせによる権利表現が可能になり、より柔軟な権利表現を可能とする。

【０１３０】

本発明に係る情報処理システムは、クライアントの保存手段に保存されている第１のライセンス情報に対して、クライアントからの要求に応じてサーバから送信された第２のライセンス情報の一部又は全部を結合し、その結合した結果のライセンス情報に基づいてクライアントがコンテンツ情報を使用するので、クライアント側では既存の権利表現に比べ、複数権利の組み合わせによる権利表現が可能になり、より柔軟な権利表現を可能とする。

【図面の簡単な説明】

【図１】

コンテンツ提供システムの一実施形態の構成図である。

【図２】

コンテンツ提供システムの一実施形態の詳細な構成図である。

【図３】

クライアントの構成を示す図である。

【図４】

サーバからクライアントへのコンテンツとライセンスの送信を示す図である。

【図５】

コンテンツとライセンスの関係を示す図である。

【図６】

クライアントの機能ブロック図である。

【図７】

サーバの機能ブロック図である。

【図８】

既存又は新規権利ファイルの構成を示す図である。

【図９】

実施例２の結合規則２－１と結合規則２－２にしたがった期間の決定処理手順を示すフローチャートである。

【図１０】

クライアントのコンテンツのダウンロード処理を説明するためのフローチャートである。

【図１１】

コンテンツサーバのコンテンツ提供処理を説明するためのフローチャートである。

【図１２】

コンテンツサーバからクライアントにコンテンツが供給される場合のコンテンツのフォーマット図である。

【図１３】

クライアントのコンテンツ再生処理を説明するためのフローチャートである。

【図１４】

クライアントのライセンス取得処理を説明するためのフローチャートである。

【図１５】

ライセンスの構成を示す図である。

【図１６】

ライセンスサーバのライセンス提供処理を説明するためのフローチャートである。

【図１７】

クライアントのライセンス更新処理を説明するためのフローチャートである。

【図１８】

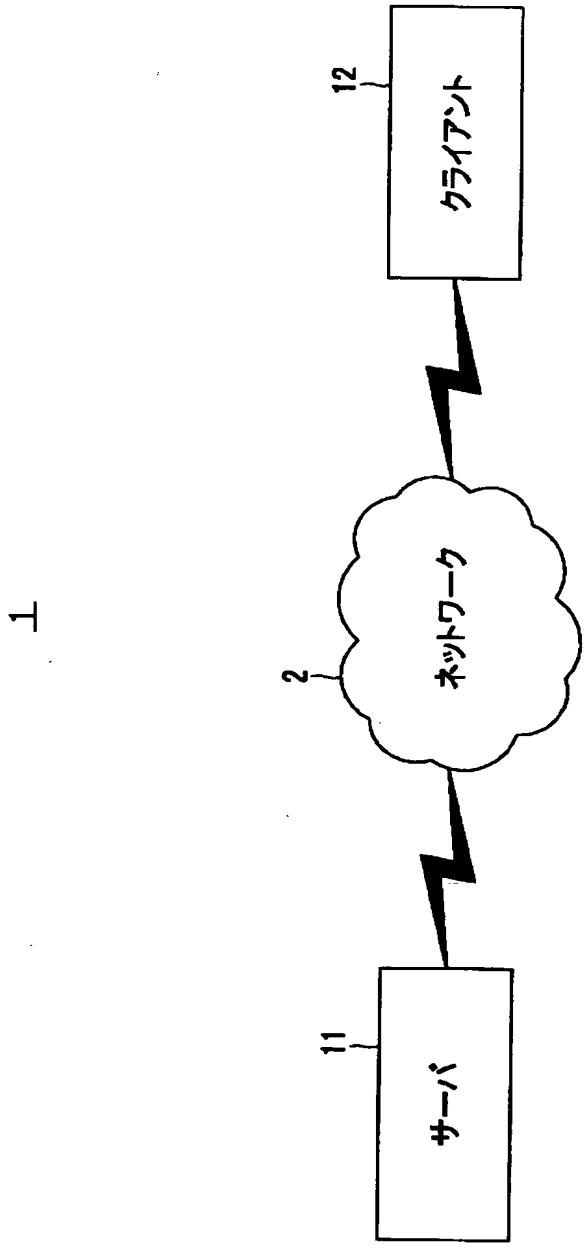
ライセンスサーバのライセンス更新処理を説明するためのフローチャートである。

【符号の説明】

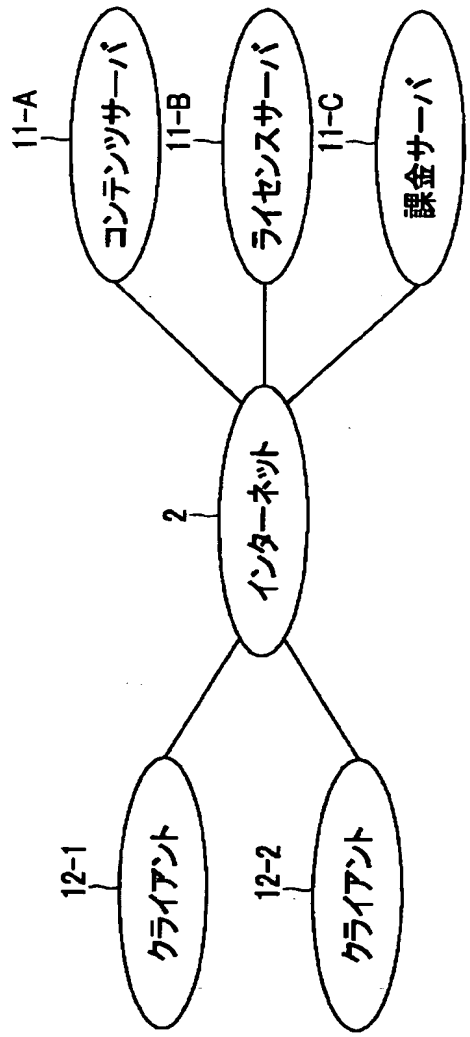
１　コンテンツ提供システム、２　ネットワーク、１２　クライアント、２１　ＣＰＵ、２８　記憶部、２９　通信部

【書類名】　図面

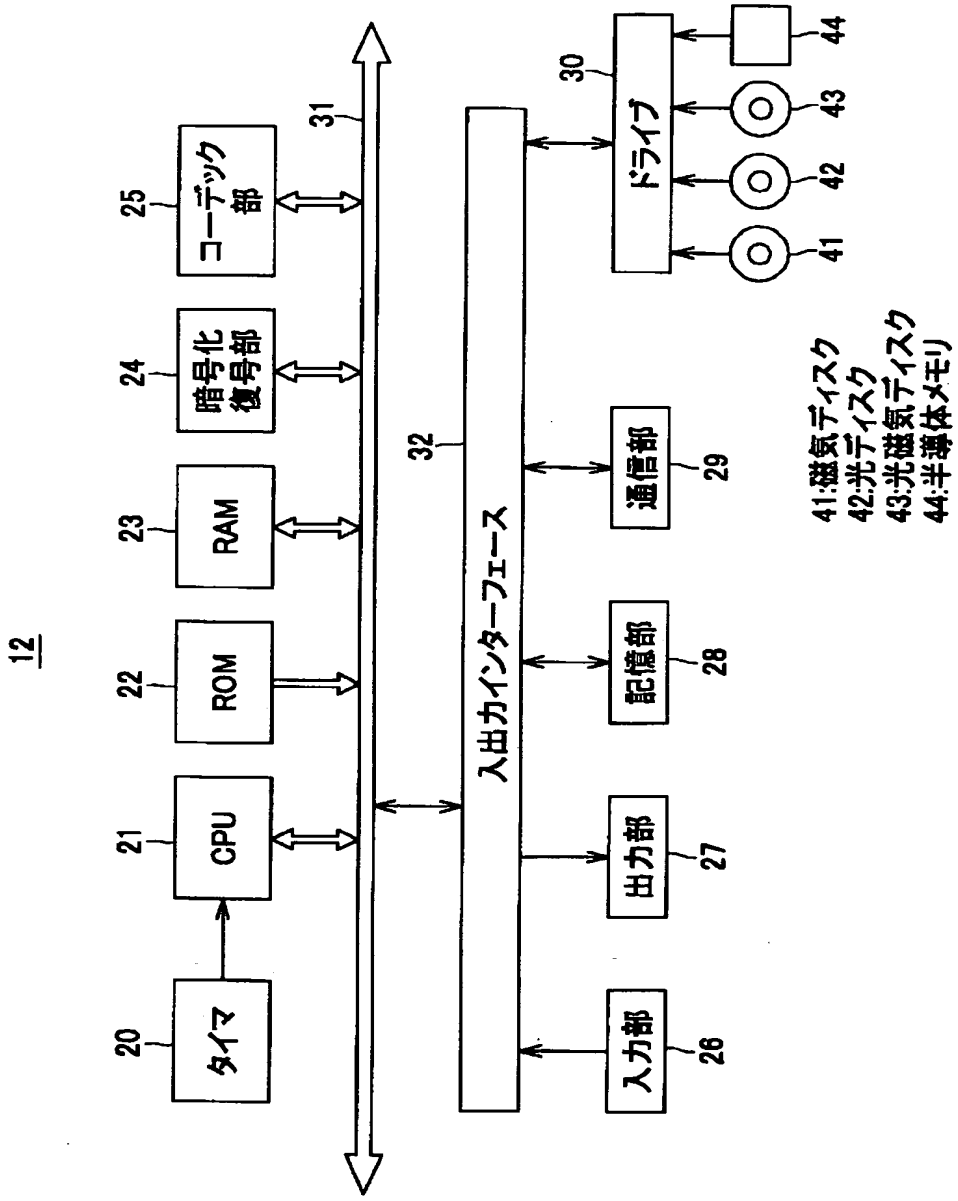
【図１】



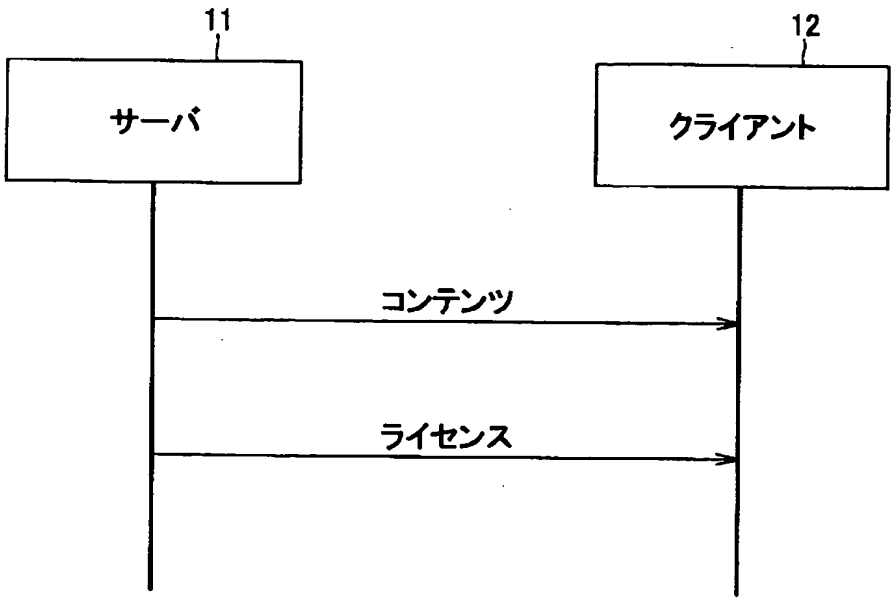
【図２】


11-A
コンテンツサーバ
11-B
ライセンスサーバ
11-C
課金サーバ
2
インターネット
12-1
クライアント
12-2
クライアント

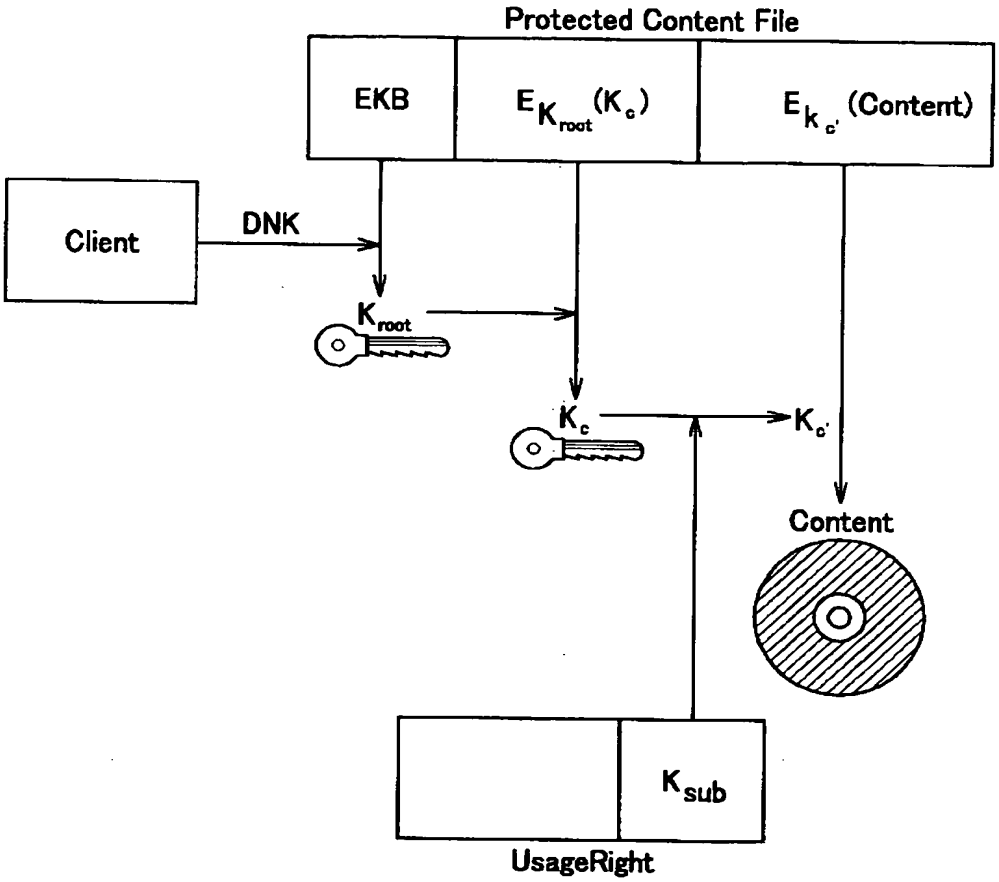
【図３】


12
20
タイマ
21
CPU
22
ROM
23
RAM
24
暗号化復号部
25
コーデック部
31
32
入出力インターフェース
26
入力部
27
出力部
28
記憶部
29
通信部
30
ドライブ
41
42
43
44
41:磁気ディスク
42:光ディスク
43:光磁気ディスク
44:半導体メモリ

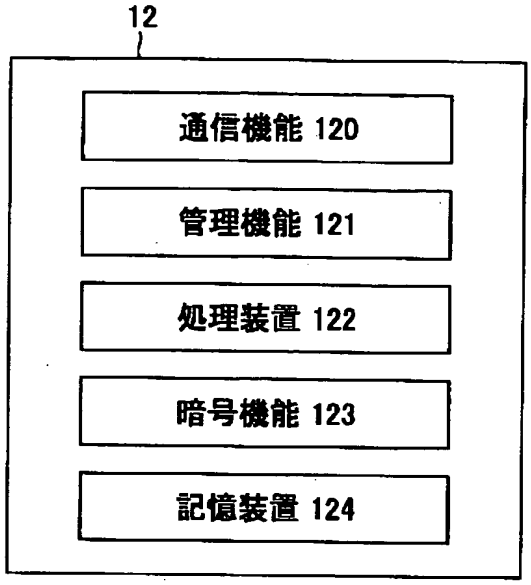
【図４】



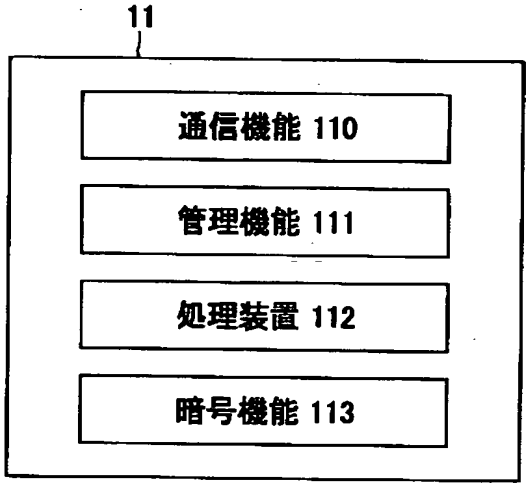
【図５】


Protected Content File
EKB
$E_{K_{root}}(K_c)$
$E_{k_{c'}}$ (Content)
Client
DNK
K_{root}
K_c
$K_{c'}$
Content
K_{sub}
UsageRight

【図６】


12
通信機能 120
管理機能 121
処理装置 122
暗号機能 123
記憶装置 124

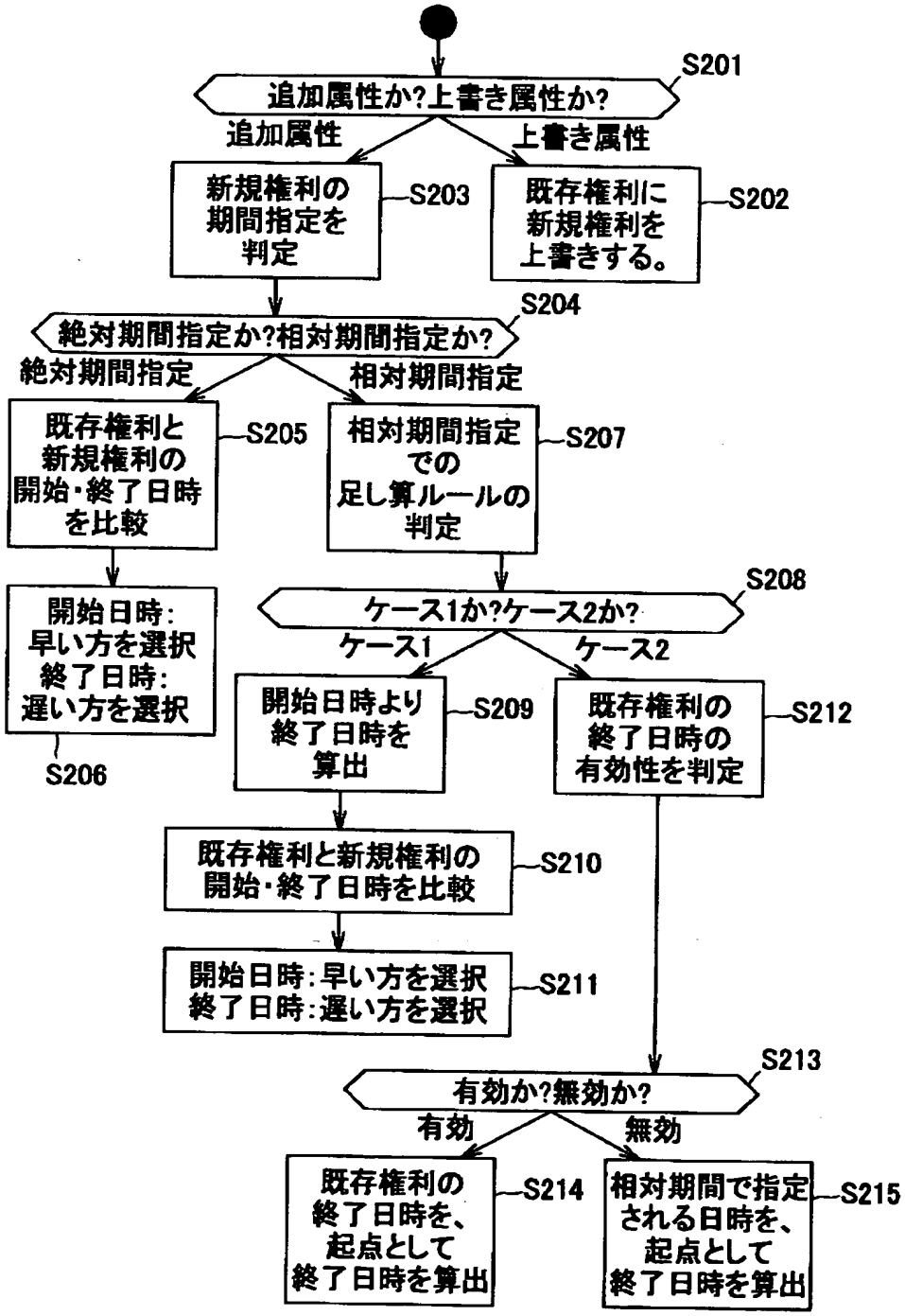
【図７】


11
通信機能 110
管理機能 111
処理装置 112
暗号機能 113

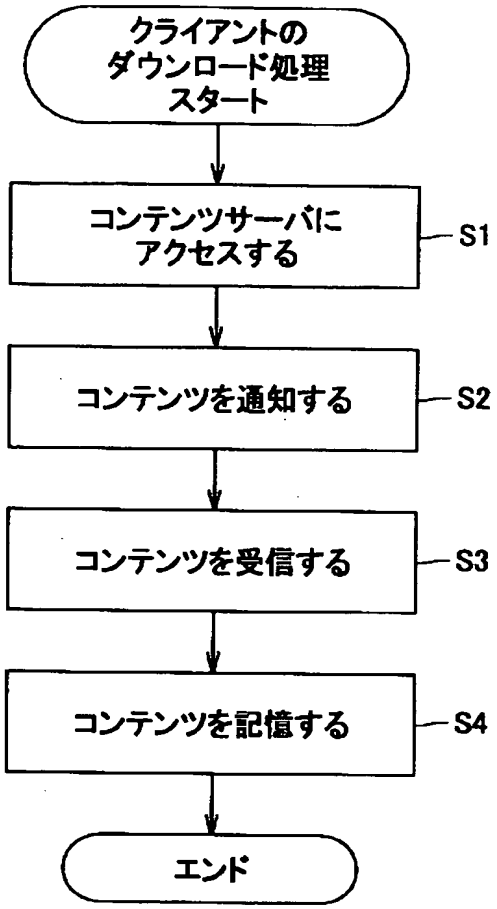
【図８】

Data Name
UsageRightType
CID
UsageRight Disjunction Rules
Leaf ID
Device and Media Categories for Check Out
Check Out Max Count
Device and Media Categories for copy
Copy Max Count
AT3CD Burn Max Count
start_time
end_time
period_time

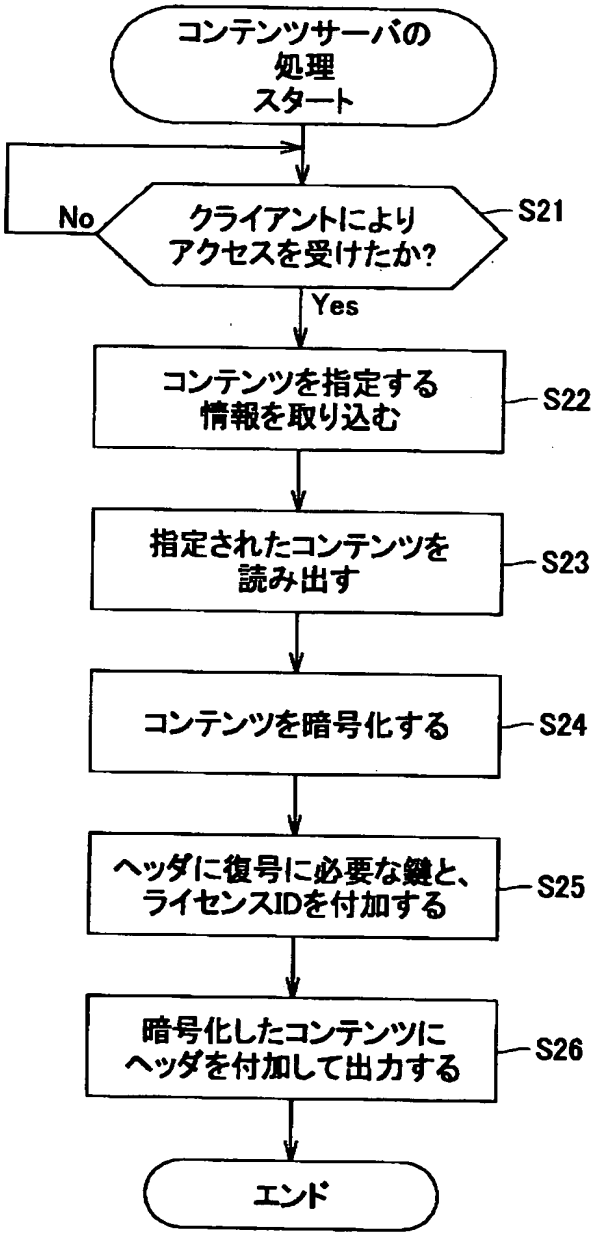
【図９】


S201
追加属性か?上書き属性か?
追加属性
上書き属性
新規権利の期間指定を判定
S203
既存権利に新規権利を上書きする。
S202
S204
絶対期間指定か?相対期間指定か?
絶対期間指定
相対期間指定
既存権利と新規権利の開始・終了日時を比較
S205
相対期間指定での足し算ルールの判定
S207
開始日時:早い方を選択
終了日時:遅い方を選択
S206
S208
ケース1か?ケース2か?
ケース1
ケース2
開始日時より終了日時を算出
S209
既存権利の終了日時の有効性を判定
S212
既存権利と新規権利の開始・終了日時を比較
S210
開始日時:早い方を選択
終了日時:遅い方を選択
S211
S213
有効か?無効か?
有効
無効
既存権利の終了日時を、起点として終了日時を算出
S214
相対期間で指定される日時を、起点として終了日時を算出
S215

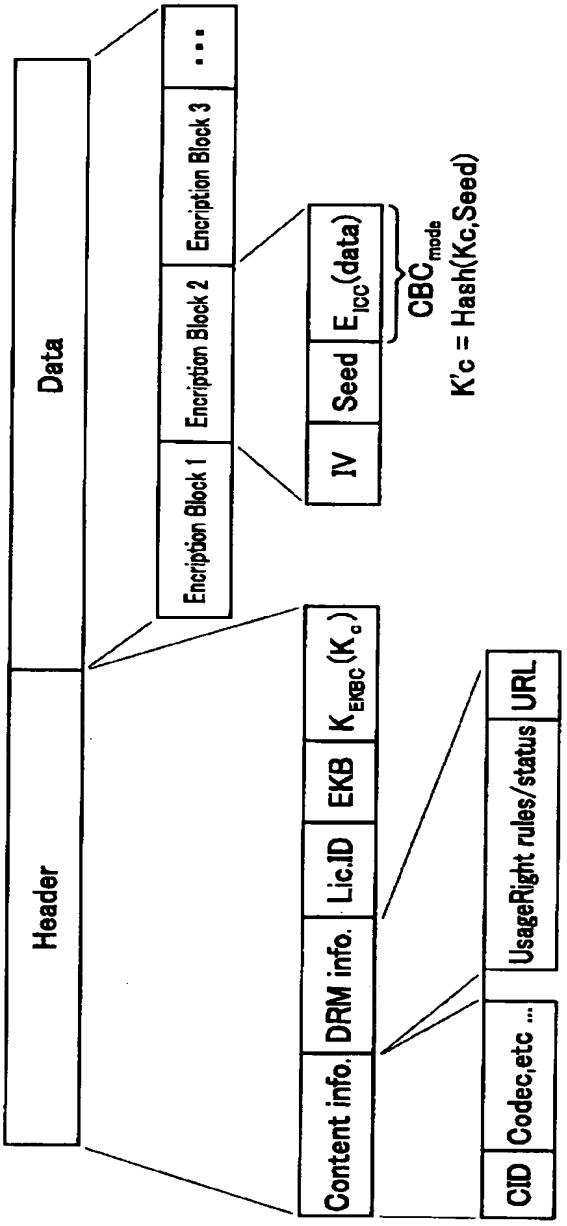
【図１０】


クライアントの
ダウンロード処理
スタート
コンテンツサーバに
アクセスする
S1
コンテンツを通知する
S2
コンテンツを受信する
S3
コンテンツを記憶する
S4
エンド

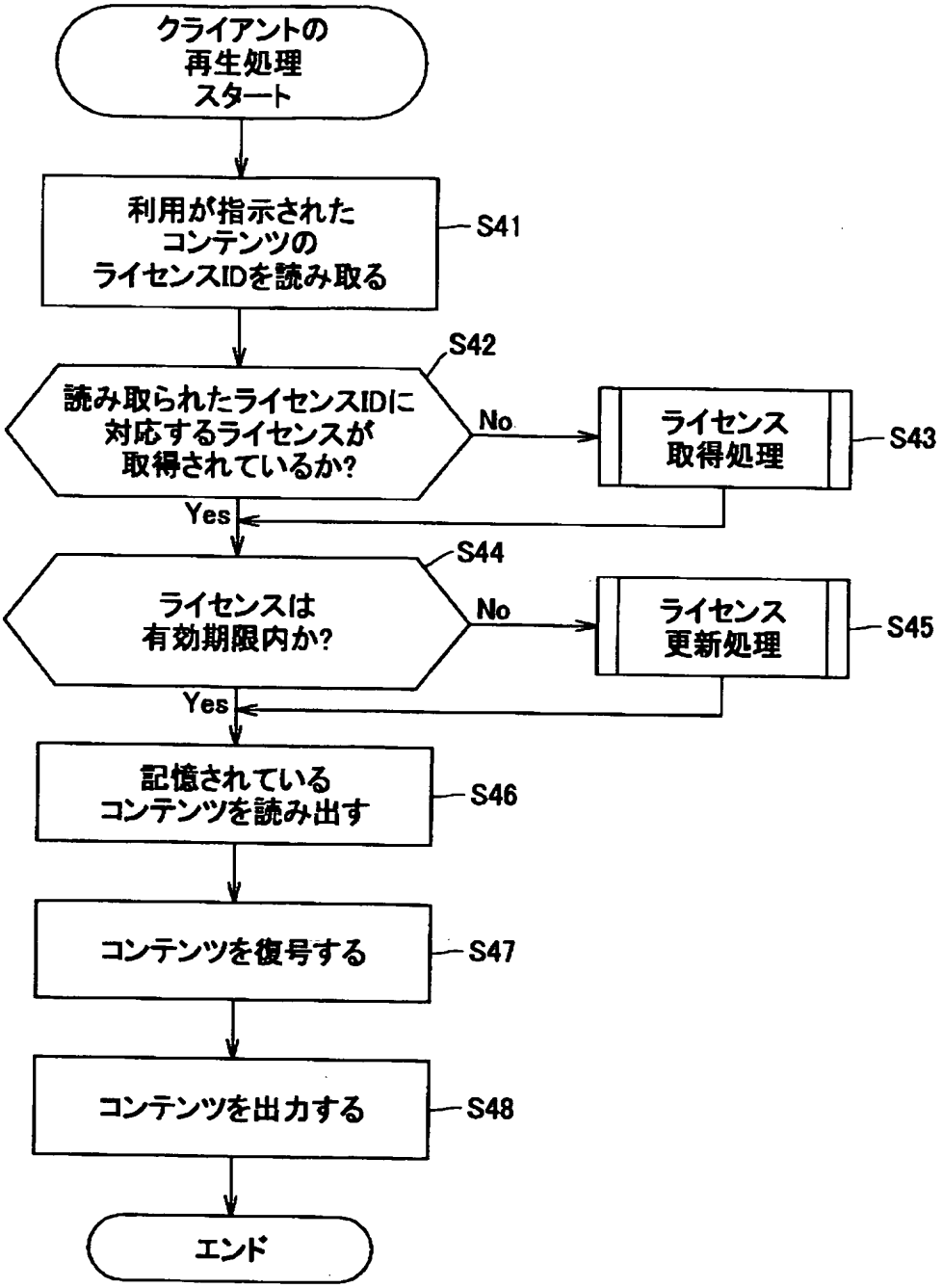
【図１１】


コンテンツサーバの
処理
スタート
No
クライアントにより
アクセスを受けたか?
S21
Yes
コンテンツを指定する
情報を取り込む
S22
指定されたコンテンツを
読み出す
S23
コンテンツを暗号化する
S24
ヘッダに復号に必要な鍵と、
ライセンスIDを付加する
S25
暗号化したコンテンツに
ヘッダを付加して出力する
S26
エンド

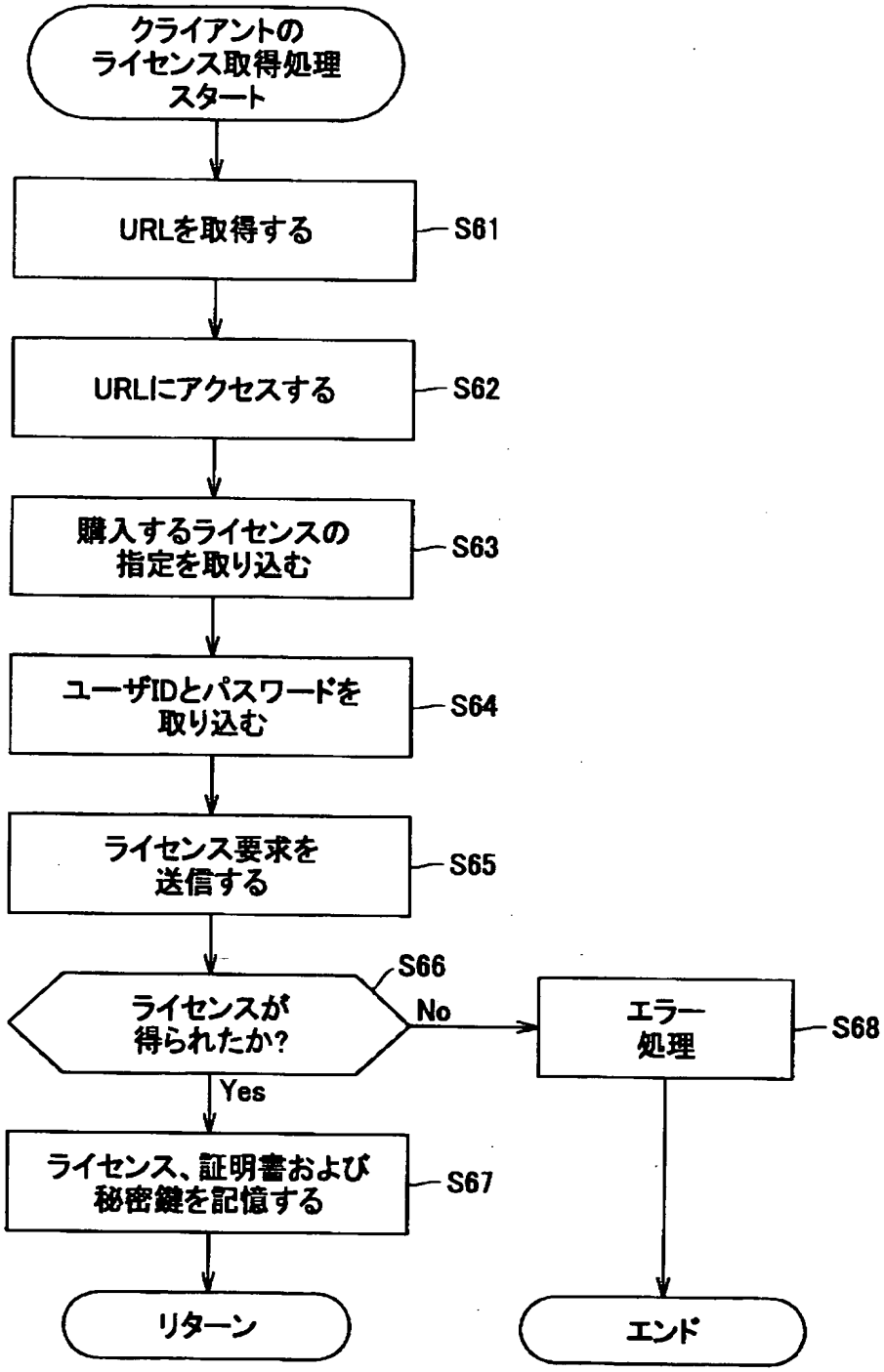
【図１２】


Header
Data
Content info.
DRM info.
Lic.ID
EKB
$K_{EKBC}(K_c)$
CID
Codec,etc ...
UsageRight rules/status
URL
Encription Block 1
Encription Block 2
Encription Block 3
...
IV
Seed
$E_{ICC}(data)$
CBC_{mode}
K'c = Hash(Kc,Seed)

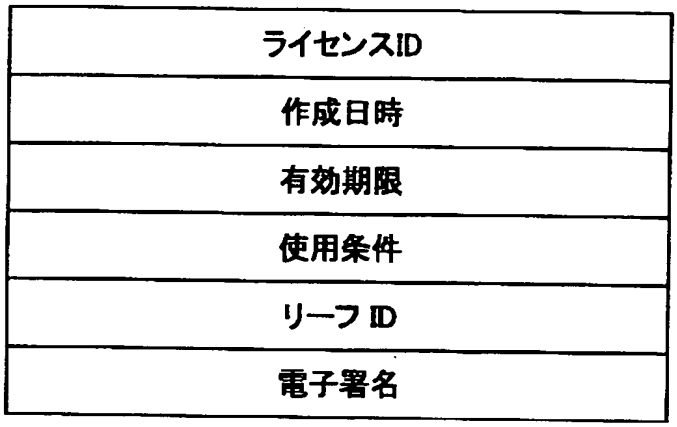
【図１３】


クライアントの
再生処理
スタート
利用が指示された
コンテンツの
ライセンスIDを読み取る
S41
S42
読み取られたライセンスIDに
対応するライセンスが
取得されているか?
No
ライセンス
取得処理
S43
Yes
S44
ライセンスは
有効期限内か?
No
ライセンス
更新処理
S45
Yes
記憶されている
コンテンツを読み出す
S46
コンテンツを復号する
S47
コンテンツを出力する
S48
エンド

【図１４】

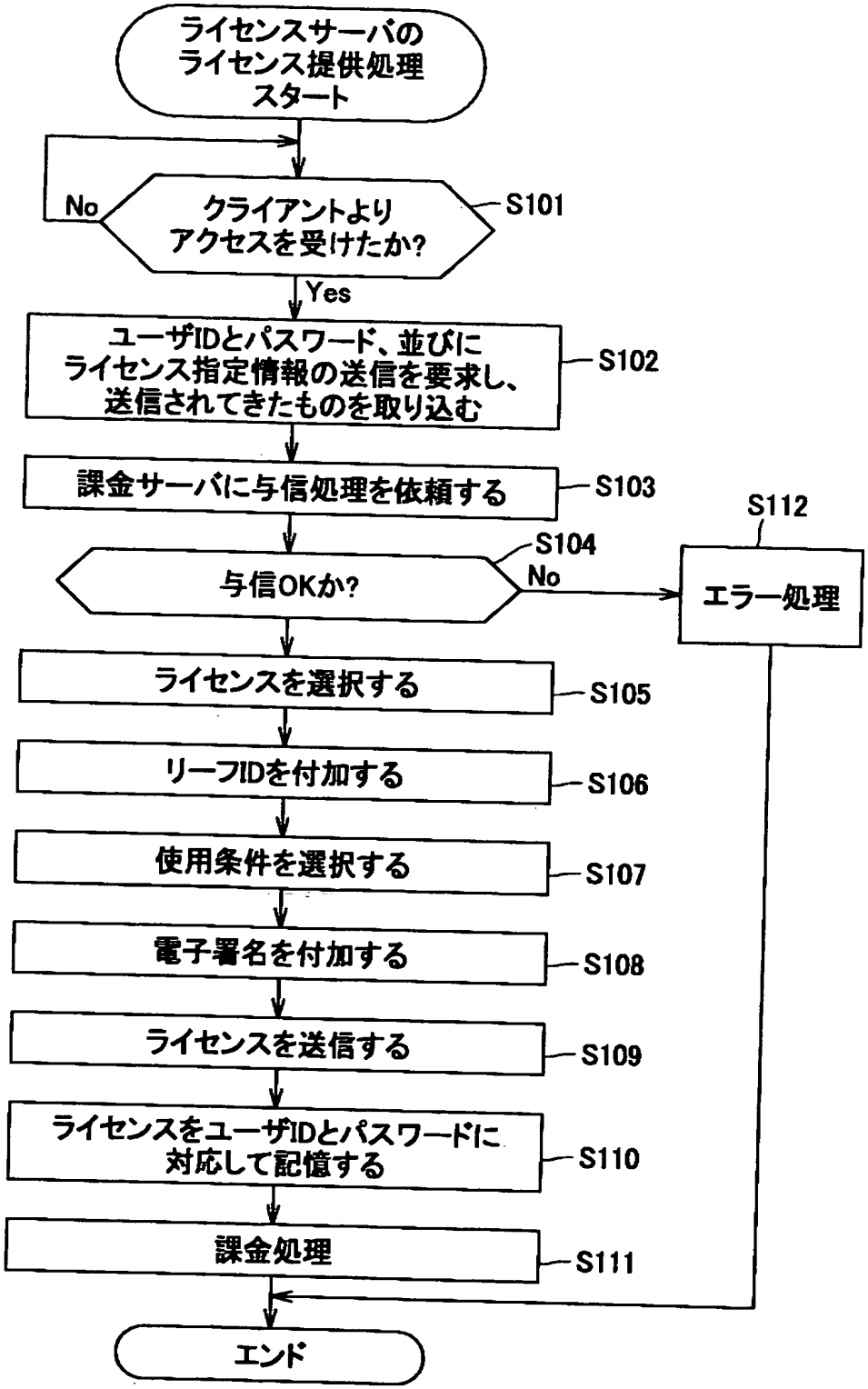

クライアントの
ライセンス取得処理
スタート
URLを取得する
S61
URLにアクセスする
S62
購入するライセンスの
指定を取り込む
S63
ユーザIDとパスワードを
取り込む
S64
ライセンス要求を
送信する
S65
S66
ライセンスが
得られたか?
No
エラー
処理
S68
Yes
ライセンス、証明書および
秘密鍵を記憶する
S67
リターン
エンド

【図１５】

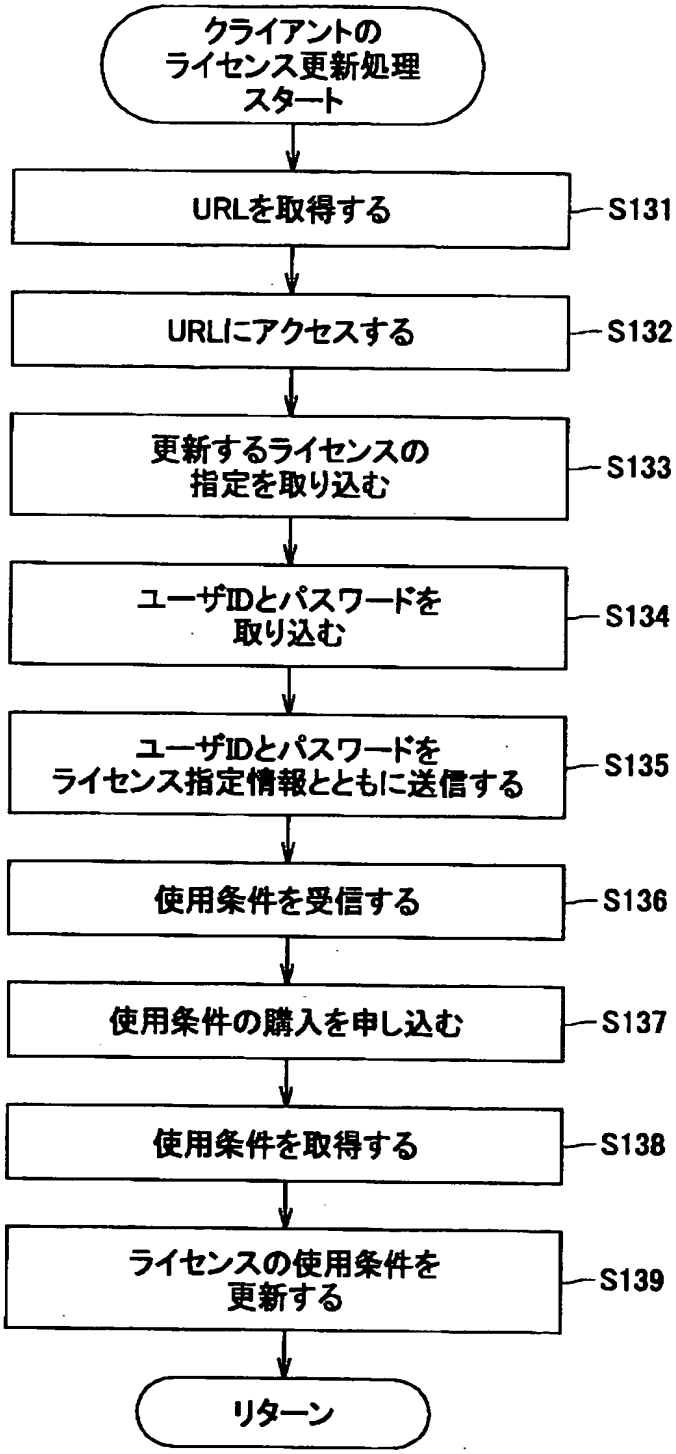


ライセンス

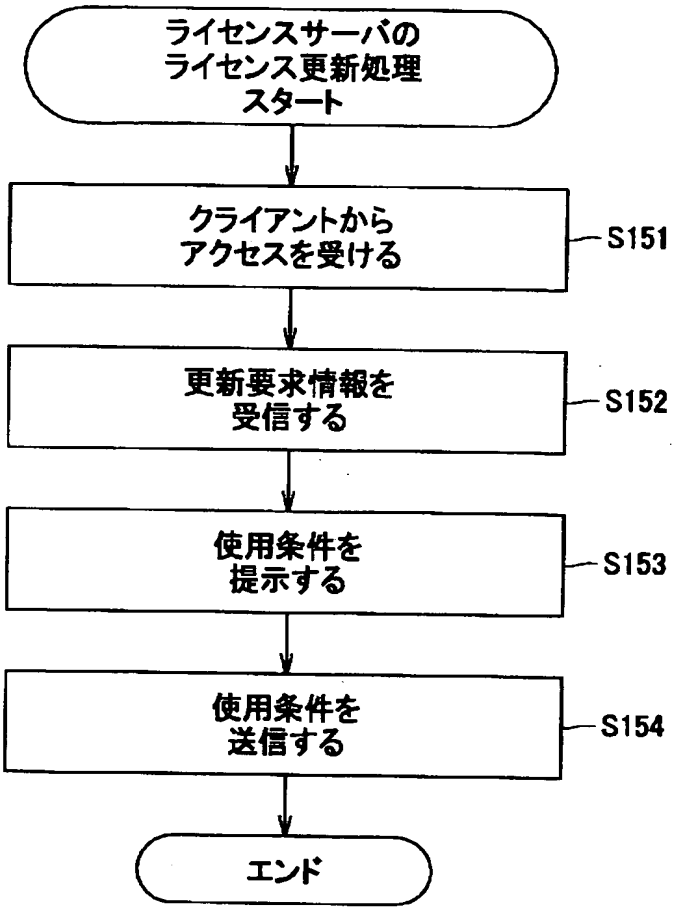
【図１６】


ライセンスサーバの
ライセンス提供処理
スタート
No
クライアントより
アクセスを受けたか?
S101
Yes
ユーザIDとパスワード、並びに
ライセンス指定情報の送信を要求し、
送信されてきたものを取り込む
S102
課金サーバに与信処理を依頼する
S103
S112
S104
与信OKか?
No
エラー処理
ライセンスを選択する
S105
リーフIDを付加する
S106
使用条件を選択する
S107
電子署名を付加する
S108
ライセンスを送信する
S109
ライセンスをユーザIDとパスワードに
対応して記憶する
S110
課金処理
S111
エンド

【図１７】


クライアントの
ライセンス更新処理
スタート
URLを取得する
S131
URLにアクセスする
S132
更新するライセンスの
指定を取り込む
S133
ユーザIDとパスワードを
取り込む
S134
ユーザIDとパスワードを
ライセンス指定情報とともに送信する
S135
使用条件を受信する
S136
使用条件の購入を申し込む
S137
使用条件を取得する
S138
ライセンスの使用条件を
更新する
S139
リターン

【図１８】


ライセンスサーバの
ライセンス更新処理
スタート
クライアントから
アクセスを受ける
S151
更新要求情報を
受信する
S152
使用条件を
提示する
S153
使用条件を
送信する
S154
エンド

【書類名】　　要約書

【要約】

【課題】　複数権利の組み合わせによる権利表現を可能とし、より柔軟な権利表現が可能とする。

【解決手段】　クライアント１２は、ライセンス情報に記された使用条件の範囲内でコンテンツ情報を使用可能な情報処理装置であり、既存（第１の）ライセンス情報を記憶部２８に記憶している。また、新規（第２の）ライセンス情報を通信部２９にて受信し、既存（第１の）ライセンス情報に対して新規（第２の）ライセンス情報の一部又は全部を結合する。この結合されたライセンス情報の範囲内でコンテンツ情報を使用する。

【選択図】　図３

特願２００３－１４２５９３

出願人履歴情報

識別番号　［０００００２１８５］

１．変更年月日　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社